

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-201169
(P2000-201169A)

(43)公開日 平成12年7月18日(2000.7.18)

(51)Int.Cl. ⁷	識別番号	F I	テマコード ⁷ (参考)
H 0 4 L 12/54		H 0 4 L 11/20	1 0 1 B 5 B 0 8 9
12/58		C 0 6 F 13/00	3 5 1 C 5 J 1 0 4
G 0 6 F 13/00	3 5 1	G 0 9 C 1/00	6 4 0 B 5 K 0 3 0
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 7 5 D 9 A 0 0 1
H 0 4 L 9/32			6 7 5 B

審査請求 有 請求項の数112 O L (全 65 頁)

(21)出願番号 特願平11-82211

(22) 出願日 平成11年3月25日(1999.3.25)

(31)優先權主張番号 特願平10-79837

(32)優先日 平成10年3月26日(1998.3.26)

(33)優先権主張国 日本 (JP)

(31)優先權主張番号 特願平10-171930

(32)優先日 平成10年6月18日(1998. 6. 18)

(33)優先権主張国 日本 (JP)

(31)優先權主張番号 特願平10-224861

(32)優先日 平成10年8月7日(1998.8.7)

(33)優先権主張国 日本 (J P)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72)発明者 久田 裕介

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 小野 諭

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 100083806

井理士 三好 秀和 (外1名)

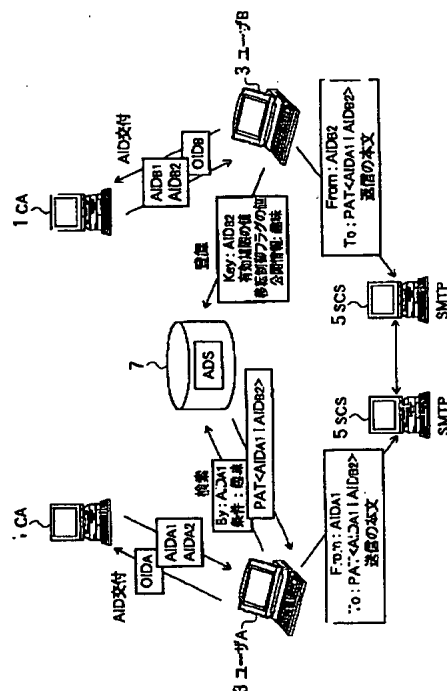
最終頁に続く

(54) 【発明の名称】 メールアクセス制御方法、通信システム、およびメールアクセス制御プログラムを格納した記憶媒体

(57) 【要約】

【課題】 匿名性とセキュリティを確保すべく発信者および着信者の匿名性を保持しつつ発信者からの通信の接続を可能とするメールアクセス制御方式を提供すること。

【解決手段】 着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取り、該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御する。また、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義し、通信ネットワーク上のメールの通信において各ユーザを各ユーザの役割識別子により識別する。



【特許請求の範囲】

【請求項1】 着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、

該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップと、
を有することを特徴とするメールアクセス制御方法。

【請求項2】 前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否することを特徴とする請求項1記載のメールアクセス制御方法。

【請求項3】 前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証することを特徴とする請求項2記載のメールアクセス制御方法。

【請求項4】 前記受け取るステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、前記制御するステップにおいて、該セキュア・コミュニケーション・サービスは発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否することを特徴とする請求項1記載のメールアクセス制御方法。

【請求項5】 前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否することを特徴とする請求項1記載のメールアクセス制御方法。

【請求項6】 前記個別化アクセスチケットの有効期限は信頼できる第三者機関により設定されたものであることを特徴とする請求項5記載のメールアクセス制御方法。

【請求項7】 各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理するディレクトリ・サービスにおいて、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者に対して前記個別化アクセスチケットを発行するステップを、更に有することを特徴とする請求項1記載のメールアクセス制御方法。

【請求項8】 そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み、該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを、予め前記セキュア・コミュニケーション・サービスに登録するステップを更に有し、

前記制御するステップにおいて、該セキュア・コミュニケーション・サービスは発信者により提示された個別化アクセスチケットがそこに予め登録されたものであるときには前記メールの配送を拒否することを特徴とする請求項1記載のメールアクセス制御方法。

【請求項9】 前記登録するステップにおいて個別化アクセスチケットに登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービスにおいて登録された個別化アクセスチケットを削除するステップを、更に有することを特徴とする請求項8記載のメールアクセス制御方法。

【請求項10】 前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービスにより発信者を認証すべきかどうかを示す移転制御フラグも含み、前記制御するステップにおいて、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、該セキュア・コミュニケーション・サービスは発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否することを特徴とする請求項1記載のメールアクセス制御方法。

【請求項11】 前記発信者識別子の認証は、発信者と前記セキュア・コミュニケーション・サービス間のチャレンジ／レスポンス認証により実現することを特徴とする請求項10記載のメールアクセス制御方法。

【請求項12】 前記個別化アクセスチケットの移転制御フラグは信頼できる第三者機関により設定されたものであることを特徴とする請求項10記載のメールアクセス制御方法。

【請求項13】 前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の実メールアドレスにより与えられることを特徴とする請求項1記載のメールアクセス制御方法。

【請求項14】 前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子

により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであることを特徴とする請求項1記載のメールアドレス制御方法。

【請求項15】 前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項14記載のメールアドレス制御方法。

【請求項16】 前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項14記載のメールアドレス制御方法。

【請求項17】 前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする請求項14記載のメールアドレス制御方法。

【請求項18】 それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられることを特徴とする請求項1記載のメールアドレス制御方法。

【請求項19】 前記各役割識別子のリンク情報は、前記認証局により各役割識別子に一意に付与された識別子であることを特徴とする請求項18記載のメールアドレス制御方法。

【請求項20】 前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする請求項18記載のメールアドレス制御方法。

【請求項21】 前記個別化アクセスチケットは、一つの発信者識別子と一つの着信者識別子を1対1に対応付けて含むことを特徴とする請求項1記載のメールアドレス制御方法。

【請求項22】 前記個別化アクセスチケットは、一つの発信者識別子と複数の着信者識別子を1対N（Nは1より大きい整数）に対応付けて含むことを特徴とする請求項1記載のメールアドレス制御方法。

【請求項23】 前記一つの発信者識別子と複数の着信者識別子の内の一識別子は前記個別化アクセスチケットの所有者を特定する所有者識別子であり、前記一つの発信者識別子と複数の着信者識別子の内の他の識別子は該

所有者が属するグループの会員を特定する会員識別子であることを特徴とする請求項22記載のメールアドレス制御方法。

【請求項24】 各ユーザの識別子と、各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnablerを認証局において各ユーザに発行して、該個別化アクセスチケットに含まれる所有者識別子と該所有者識別子に対応するEnablerの両方をセキュアな演算装置に対して提示したユーザによってのみ該セキュアな演算装置において該個別化アクセスチケットに対する所定の演算を行えるようにするステップを、更に有することを特徴とする請求項23記載のメールアドレス制御方法。

【請求項25】 前記認証局は、それがEnablerであることを示す情報と各ユーザの識別子の実体に対し、該認証局の秘密鍵で署名したものを各ユーザの識別子のEnablerとして発行することを特徴とする請求項24記載のメールアドレス制御方法。

【請求項26】 前記所定の演算は、個別化アクセスチケットの新規作成、複数個別化アクセスチケットのマージ、一個別化アクセスチケットの複数個別化アクセスチケットへの分割、個別化アクセスチケットの所有者変更、個別化アクセスチケットの有効期限の変更、個別化アクセスチケットの移転制御フラグの変更、を含むことを特徴とする請求項24記載のメールアドレス制御方法。

【請求項27】 すべてのユーザに既知である特殊な識別子と該特殊な識別子に対応する特殊なEnablerを定義して、前記個別化アクセスチケットの新規生成および前記個別化アクセスチケットの所有者変更を、前記個別化アクセスチケットの所有者が、該特殊な識別子および該特殊なEnablerを用いて会員識別子のEnablerを使わずに行えるようにすることを特徴とする請求項26記載のメールアドレス制御方法。

【請求項28】 前記特殊な識別子は、個別化アクセスチケットの所有者識別子としてのみ使用可能であるように定義されていることを特徴とする請求項27記載のメールアドレス制御方法。

【請求項29】 すべてのユーザに既知である特殊な識別子を定義して、該特殊な識別子を用いて個別化アクセスチケットに読取専用属性を設定できるようにすることを特徴とする請求項26記載のメールアドレス制御方法。

【請求項30】 前記制御するステップにおいて、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、前記セキュア・コミュニケーション・サービスは、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメー

ル転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すことを特徴とする請求項1記載のメールアクセス制御方法。

【請求項31】 それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義し、通信ネットワーク上のメールの通信において各ユーザを各ユーザの役割識別子により識別する、ことを特徴とするメールアクセス制御方法。

【請求項32】 前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項31記載のメールアクセス制御方法。

【請求項33】 前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項31記載のメールアクセス制御方法。

【請求項34】 着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子と着信者の役割識別子を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップ、を更に有することを特徴とする請求項31記載のメールアクセス制御方法。

【請求項35】 前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする請求項33記載のメールアクセス制御方法。

【請求項36】 前記定義するステップは、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報も定義し、各役割識別子は各役割識別子のリンク情報も含むことを特徴とする請求項31記載のメールアクセス制御方法。

【請求項37】 前記各役割識別子のリンク情報は、前記認証局により各役割識別子に一意に付与された識別子であることを特徴とする請求項36記載のメールアクセス制御方法。

【請求項38】 着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提

示され、発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、

該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップ、を更に有することを特徴とする請求項36記載のメールアクセス制御方法。

【請求項39】 前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする請求項38記載のメールアクセス制御方法。

【請求項40】 複数のユーザ端末が接続された通信網と、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、該通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービス装置と、を有することを特徴とするメールアクセス制御を実現した通信システム。

【請求項41】 前記セキュア・コミュニケーション・サービス装置は発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否することを特徴とする請求項40記載の通信システム。

【請求項42】 前記個別化アクセスチケットを自身の秘密鍵により署名して発行するセキュアな演算装置を更に有し、

前記セキュア・コミュニケーション・サービス装置は該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証することを特徴とする請求項41記載の通信システム。

【請求項43】 前記セキュア・コミュニケーション・サービス装置は発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれ

ていないときには、前記メールの配送を拒否することを特徴とする請求項40記載の通信システム。

【請求項44】 前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記セキュア・コミュニケーション・サービス装置は発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否することを特徴とする請求項40記載の通信システム。

【請求項45】 前記個別化アクセスチケットの有効期限を設定する信頼できる第三者機関を更に有することを特徴とする請求項44記載の通信システム。

【請求項46】 各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者に対して前記個別化アクセスチケットを発行するディレクトリ・サービス装置を更に有することを特徴とする請求項40記載の通信システム。

【請求項47】 前記セキュア・コミュニケーション・サービス装置は、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め登録し、発信者により提示された個別化アクセスチケットがそこに予め登録されたものであるときには前記メールの配送を拒否することを特徴とする請求項40記載の通信システム。

【請求項48】 前記セキュア・コミュニケーション・サービス装置は、前記個別化アクセスチケットを登録した前記特定の登録者からの要求により、そこに登録された個別化アクセスチケットを削除することを特徴とする請求項47記載の通信システム。

【請求項49】 前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービス装置により発信者を認証すべきかどうかを示す移転制御フラグも含み、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、該セキュア・コミュニケーション・サービス装置は発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否することを特徴とする請求項40記載の通信システム。

【請求項50】 前記発信者識別子の認証は、発信者と前記セキュア・コミュニケーション・サービス装置間のチャレンジ/レスポンス認証により実現することを特徴とする請求項49記載の通信システム。

【請求項51】 前記個別化アクセスチケットの移転制

御フラグを設定する信頼できる第三者機関を更に有することを特徴とする請求項49記載の通信システム。

【請求項52】 前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の実メールアドレスにより与えられることを特徴とする請求項40記載の通信システム。

【請求項53】 それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子を発行する認証局装置を更に有し、

前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられることを特徴とする請求項40記載の通信システム。

【請求項54】 前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする請求項53記載の通信システム。

【請求項55】 前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする請求項53記載の通信システム。

【請求項56】 前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする請求項53記載の通信システム。

【請求項57】 それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とを発行する認証局装置を更に有し、

前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられることを特徴とする請求項40記載の通信システム。

【請求項58】 前記各役割識別子のリンク情報は、前記認証局装置により各役割識別子に一意に付与された識別子であることを特徴とする請求項57記載の通信システム。

【請求項59】 前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする請求項57記載の通信システム。

【請求項60】 前記個別化アクセスチケットは、一つ

の発信者識別子と一つの着信者識別子を1対1に対応付けて含むことを特徴とする請求項40記載の通信システム。

【請求項61】 前記個別化アクセスチケットは、一つの発信者識別子と複数の着信者識別子を1対N（Nは1より大きい整数）に対応付けて含むことを特徴とする請求項40記載の通信システム。

【請求項62】 前記一つの発信者識別子と複数の着信者識別子の内の一識別子は前記個別化アクセスチケットの所有者を特定する所有者識別子であり、前記一つの発信者識別子と複数の着信者識別子の内の他の識別子は該所有者が属するグループの会員を特定する会員識別子であることを特徴とする請求項61記載の通信システム。

【請求項63】 各ユーザの識別子と、各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnablerを各ユーザに発行する認証局装置と、該個別化アクセスチケットに含まれる所有者識別子と該所有者識別子に対応するEnablerの両方を提示したユーザによってのみ該個別化アクセスチケットに対する所定の演算を行うことを可能としたセキュアな演算装置と、を更に有することを特徴とする請求項62記載の通信システム。

【請求項64】 前記認証局装置は、それがEnablerであることを示す情報と各ユーザの識別子の実体に対し、該認証局の秘密鍵で署名したものを各ユーザの識別子のEnablerとして発行することを特徴とする請求項63記載の通信システム。

【請求項65】 前記所定の演算は、個別化アクセスチケットの新規作成、複数個別化アクセスチケットのマージ、一個別化アクセスチケットの複数個別化アクセスチケットへの分割、個別化アクセスチケットの所有者変更、個別化アクセスチケットの有効期限の変更、個別化アクセスチケットの移転制御フラグの変更、を含むことを特徴とする請求項63記載の通信システム。

【請求項66】 すべてのユーザに既知である特殊な識別子と該特殊な識別子に対応する特殊なEnablerを定義して、前記個別化アクセスチケットの新規生成および前記個別化アクセスチケットの所有者変更を、前記個別化アクセスチケットの所有者が、該特殊な識別子および該特殊なEnablerを用いて会員識別子のEnablerを使わずに行えるようにしたことを特徴とする請求項65記載の通信システム。

【請求項67】 前記特殊な識別子は、個別化アクセスチケットの所有者識別子としてのみ使用可能であるように定義されていることを特徴とする請求項66記載の通信システム。

【請求項68】 すべてのユーザに既知である特殊な識別子を定義して、該特殊な識別子を用いて個別化アクセスチケットに読取専用属性を設定できるようにしたこと

を特徴とする請求項65記載の通信システム。

【請求項69】 前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、前記セキュア・コミュニケーション・サービス装置は、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すことを特徴とする請求項40記載の通信システム。

【請求項70】 それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義する認証局装置と、そこでのメールの通信において各ユーザが各ユーザの役割識別子により識別される通信網と、を有することを特徴とするメールアクセス制御を実現した通信システム。

【請求項71】 前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする請求項70記載の通信システム。

【請求項72】 前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項70記載の通信システム。

【請求項73】 着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子と着信者の役割識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、前記通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービス装置を更に有することを特徴とする請求項70記載の通信システム。

【請求項74】 前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする請求項73記載の通信システム。

【請求項75】 前記認証局装置は、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報も定義し、各役割識別子は各役割識別子のリンク情報も含むことを特徴とする請求項70記載の通信システム。

【請求項76】 前記各役割識別子のリンク情報は、前

記認証局装置により各役割識別子に一意に付与された識別子であることを特徴とする請求項75記載の通信システム。

【請求項77】 着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、前記通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスを更に有することを特徴とする請求項75記載の通信システム。

【請求項78】 前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする請求項77記載の通信システム。

【請求項79】 コンピュータハードウェアと、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子に対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、発信者と着信者間の通信を接続するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュア・コミュニケーション・サービス装置。

【請求項80】 前記コンピュータソフトウェアは、発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項79記載のセキュア・コミュニケーション・サービス装置。

【請求項81】 前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記コンピュータソフトウェアは、該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証するように前記コンピュータハードウェアを動作させることを特徴とする請求項80記載のセキュア・コミュニケーション・サービス装置。

【請求項82】 前記コンピュータソフトウェアは、発信者により前記個別化アクセスチケットと共に提示され

た発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項79記載のセキュア・コミュニケーション・サービス装置。

【請求項83】 前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記コンピュータソフトウェアは、発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項79記載のセキュア・コミュニケーション・サービス装置。

【請求項84】 前記コンピュータソフトウェアは、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め前記セキュア・コミュニケーション・サービスに登録し、発信者により提示された個別化アクセスチケットが前記セキュア・コミュニケーション・サービスに予め登録されたものであるときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項79記載のセキュア・コミュニケーション・サービス装置。

【請求項85】 前記コンピュータソフトウェアは、個別化アクセスチケットに登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービスにおいて登録された個別化アクセスチケットを削除するように前記コンピュータハードウェアを動作させることを特徴とする請求項84記載のセキュア・コミュニケーション・サービス装置。

【請求項86】 前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービスにより発信者を認証すべきかどうかを示す移転制御フラグも含み、前記コンピュータソフトウェアは、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項79記載のセキュア・コミュニケーション・サービス装置。

【請求項87】 前記コンピュータソフトウェアは、前記発信者識別子の認証を、発信者と前記セキュア・コミュニケーション・サービス間のチャレンジ/レスポンス

認証により実現するように前記コンピュータハードウェアを動作させることを特徴とする請求項86記載のセキュア・コミュニケーション・サービス装置。

【請求項88】 前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであって、前記コンピュータソフトウェアは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータハードウェアを動作させることを特徴とする請求項79記載のセキュア・コミュニケーション・サービス装置。

【請求項89】 それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられ、前記コンピュータソフトウェアは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータハードウェアを動作させることを特徴とする請求項79記載のセキュア・コミュニケーション・サービス装置。

【請求項90】 前記コンピュータソフトウェアは、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すように前記コンピュータハードウェアを動作させることを特徴とする請求項79記載のセキュア・コミュニケーション・サービス装置。

【請求項91】 コンピュータハードウェアと、個別化アクセスチケットの要求をユーザから受け取り、発信者識別子と着信者識別子に対応付けて含み、自身の秘密鍵により署名された個別化アクセスチケットを発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置。

【請求項92】 コンピュータハードウェアと、

各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者に対して、発信者から指定された検索条件に応じて、検索条件を満たした非個人的公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるディレクトリ・サービス装置。

【請求項93】 コンピュータハードウェアと、それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を、各ユーザに対して発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおける認証局装置。

【請求項94】 コンピュータハードウェアと、各ユーザの識別子と、一般に一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの中で該各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnable r を各ユーザに対して発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおける認証局装置。

【請求項95】 コンピュータハードウェアと、一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの要求をユーザから受け取り、該ユーザが該個別化アクセスチケットに含まれる所有者識別子と該ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示し該所有者識別子に対応するEnabler の両方を提示したときに該個別化アクセスチケットに対する所定の演算を行うように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、

を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置。

【請求項96】 着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子に対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを

制御して、発信者と着信者間の通信を接続する、メールアクセス制御を実現した通信システムにおけるセキュア・コミュニケーション・サービス装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項 97】 前記プログラムは、発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項 96 記載の記憶媒体。

【請求項 98】 前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記プログラムは、該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証するように前記コンピュータを動作させることを特徴とする請求項 97 記載の記憶媒体。

【請求項 99】 前記プログラムは、発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項 96 記載の記憶媒体。

【請求項 100】 前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記プログラムは、発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項 96 記載の記憶媒体。

【請求項 101】 前記プログラムは、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め前記セキュア・コミュニケーション・サービス装置に登録し、発信者により提示された個別化アクセスチケットが前記セキュア・コミュニケーション・サービス装置に予め登録されたものであるときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項 96 記載の記憶媒体。

【請求項 102】 前記プログラムは、個別化アクセスチケットに登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービス装置において登録された個別化アクセスチケットを削除するように前記コンピュータを動作させることを特徴とする

請求項 101 記載の記憶媒体。

【請求項 103】 前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービス装置により発信者を認証すべきかどうかを示す移転制御フラグも含み、前記プログラムは、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項 96 記載の記憶媒体。

【請求項 104】 前記プログラムは、前記発信者識別子の認証を、発信者と前記セキュア・コミュニケーション・サービス装置間のチャレンジ/レスポンス認証により実現するように前記コンピュータを動作させることを特徴とする請求項 103 記載の記憶媒体。

【請求項 105】 前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであって、前記プログラムは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータを動作させることを特徴とする請求項 96 記載の記憶媒体。

【請求項 106】 それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられ、前記プログラムは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータを動作させることを特徴とする請求項 96 記載の記憶媒体。

【請求項 107】 前記プログラムは、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すように前記コンピュータを動作させることを特徴とする請求項 96 記載の記憶媒体。

【請求項 108】 個別化アクセスチケットの要求をユ

ーザから受け取り、発信者識別子と着信者識別子を対応付けて含み、自身の秘密鍵により署名された個別化アクセスチケットを発行する、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項109】 各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者に対して、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを発行する、メールアクセス制御を実現した通信システムにおけるディレクトリ・サービス装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項110】 それにより自身が各ユーザを一意的に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を、各ユーザに対して発行する、メールアクセス制御を実現した通信システムにおける認証局装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項111】 各ユーザの識別子と、一般に一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの中で各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnablerを各ユーザに対して発行する、メールアクセス制御を実現した通信システムにおける認証局装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項112】 一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの要求をユーザから受け取り、該ユーザが該個別化アクセスチケットに含まれる所有者識別子と該ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示し該所有者識別子に対応するEnablerの両方を提示したときに該個別化アクセスチケットに対する所定の演算を行う、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、通信網において着信者の通信網における識別子を隠蔽しつつ、通信網における識別子を隠蔽した他のユーザからの通信の接続を制御してメールの送受信を制御するメールアクセス接続制御方法、通信システム、およびメールアクセス制御プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】 インターネットの普及に伴い、メールを用いたSPAMや嫌がらせ行為が急増している。SPAMとは受信者の時間的、経済的、精神的負担を考慮せず一方的に送り付けられるメールまたはニュースの総称である。メールによるSPAMはUBE(Unsolicited Bulk Email)またはUCE(Unsolicited Commercial Email)とも呼ばれている。

【0003】 SPAMは受信者の年齢、性別、嗜好等を考慮せず無差別に送信されるため、受信者にとって興味のない内容や不快な内容である場合が少なくない。受信に要する時間的負担や経済的負担も小さくない。ビジネスユーザにとっては、重要なメールがSPAMに埋もれて見つかりにくくなるため業務効率の低下を招きかねない。また、大量のユーザ宛に送信されるためネットワーク資源を浪費し、最悪の場合には過負荷を引き起こす。その結果、ユーザにとって重要なメールが失われる場合もある。また、匿名でまたは他人に成りすまして送信されるため、苦情対応のために人的資源を確保しなければならない。

【0004】 一方、嫌がらせとは特定のユーザに対し精神的苦痛を与えたり、経済的、時間的負担を負わせるために、ユーザにとって不快な内容のメールを継続的に送り続ける行為である。SPAMと同様に、実在または架空の第三者に成りすまして送信されるため、送信者の特定は極めて困難である。また、大容量メールを送り付けられたり、短時間に大量のメールを送り付けられたりするため、システムダウンの危険性もある。

【0005】 SPAMや嫌がらせ行為に対し、メールシステムは以下の要件を満足することが必要である。

【0006】 ・安全性

送信者の成りすましを検出し、配送を拒否することが必要である。

【0007】 ・堅牢性

大容量メールによるシステムダウンを回避するために、メール容量を制限することが必要である。また、大量送信によるシステムダウンを回避するために、送信回数を制限することが必要である。

【0008】 ・互換性

既存のメールシステムの実装を大きく変更しないことが必要である。

【0009】 ・操作性

既存のメールシステムの操作性を大きく変更しないことが必要である。

【0010】 sendmail, qmail等のMTA(Message Transfer Agent)はエンベロープ情報及びヘッダ情報の偽造を検出し、配送を拒否する。また、MAPS RBL等のいわゆるブラックリストを参照して、SPAMの発信源となっているメールサーバからの受信を拒否する。また、PGP, S/MIME, TLS等を用いて署名確認を行うことにより他人の実メールアドレスを騙った送信を検出し、配送を拒

否する。また、本文の部分的削除によってメッセージ長を制限する。

【0011】

【発明が解決しようとする課題】従来のメールシステムにおける実メールアドレスには以下のような問題点がある。

【0012】・身元を推測可能

実メールアドレスは身元を推測する上で有益な情報を含むため、嫌がらせの相手を選択することができる。例えば、実ドメインから勤務先を特定できる。また、ユーザ名から性別や氏名を推測することができる。

【0013】・身元から推測可能

実メールアドレスはユーザ名@ドメイン名の形式で統一されているため、実メールアドレスを知らなくても、身元さえわかれば推測できる。例えば、氏名がわかればユーザ名の候補を絞り込むことができる。また、所属組織がわかればドメイン名の候補を絞り込むことができる。また、ユーザ名を実名とは無関係な文字列で与えている場合でも、ユーザ名の命名規則がわかれば試行錯誤的な送信によって推測できる。

【0014】・移転可能

実メールアドレスは人から人に移転できるため、持ち主から直接教えてもらえなくても送信できる。メールを介した移転には以下の場合がある。他人の実メールアドレスをcc:行に指定すれば、To:行に指定したすべての受信者に移転することができる。また、第三者の実メールアドレスをReply-To:行に指定し、To:行に指定した受信者の実メールアドレスを本文に含むメールをフォワードすれば、その実メールアドレスを第三者に移転することができる。

【0015】・取り消し困難

SPAMや嫌がらせだけでなく重要なメールもよめなくなるため、実メールアドレスの取り消しは困難である。

【0016】匿名リメーラ (anonymous remailers) と呼ばれる Cypherpunk remailers と Mixmaster remailers は送信者の実メールアドレス及び実ドメインを暗号化してから配送する。この方法はreply blockと呼ばれている。reply blockの暗号化及び復号化には匿名リメーラの公開鍵及び秘密鍵を用いるため、送信者以外のいかなるユーザも送信者の実メールアドレス及び実ドメインを特定することは困難である。

【0017】匿名リメーラは実メールアドレスを特定困難なため、実メールアドレスの移転も困難である。しかしながら、reply block は移転可能であるため、受信者以外のユーザからも送信者に対し返信することが可能である。

【0018】偽名サーバ (pseudonymous server) と呼ばれる AS-Node と nym.alias.net はユーザの実メールアドレスと一意に対応した偽名アカウントを用いてメール

を送受信する。偽名アカウントはユーザ側で任意に作成できるため、ユーザは実メールアドレスを推測困難な偽名アカウントを持つことが可能である。さらに、reply block の利用により、ユーザの実メールアドレス及び実ドメインを偽名サーバに対し隠蔽することも可能である。これらの手段を組み合わせることによって、送信者以外のいかなるユーザも送信者の実メールアドレス及び実ドメインを特定することは困難となる。また、偽名アカウントは取り消し可能なため、実メールアドレスを取り消す必要もない。

【0019】偽名サーバは実メールアドレスを特定困難なため、実メールアドレスの移転も困難である。しかしながら、偽名アカウントは移転可能なため、受信者以外のユーザからも送信することが可能である。

【0020】さらに、SPAMや嫌がらせ行為から受信者を保護するためには、これらの行為を行う発信者からの接続要求を拒否することも必要である。このため、通信システムは発信者の身元を一意に特定可能であることも必要である。

【0021】これらのことから、通信システムはユーザの実メールアドレスを隠蔽しつつ（すなわち、ユーザの匿名性を保証しつつ）、そのユーザの身元を一意に特定可能であることが求められるが、従来の通信システムにおいて、これらの両者を同時に実現することは困難であった。

【0022】メールシステムにおいてユーザの身元を特定するためには、そのユーザの実メールアドレスが必要である。一方、匿名リメーラは、発信者の匿名性保証のために発信者の実メールアドレスを暗号化または削除してから配送する。

【0023】この条件において発信者の身元を特定するためには、トラフィック解析によってメールの配送経路を追跡することが必要である。ところが、匿名リメーラはメールの配送を遅らせたり、配送順序を入れ替えたりする。また、Mixmaster remailers はメールを複数のブロックに分割してから配送する。このため、トラフィック解析による配送経路の追跡は困難であり、発信者の身元特定も困難である。

【0024】偽名サーバもメールの配送において匿名リメーラを利用するため、発信者の匿名性は保証できるけれども発信者の身元を一意に特定することは困難である。

【0025】一方、ドイツ電子署名法は、通信サービスで用いられるデジタル署名を生成するためのデジタル証明書に対し、実名に加えて偽名の記入も許可している。デジタル証明書はユーザに対し一意に付与されるため、偽名を記載してもユーザの身元を一意に特定することが可能である。また、偽名の命名権はユーザ側にあるため、実名を推測困難な偽名を記載することが可能である。

【0026】本発明は、上記に鑑みてなされたもので、その目的とするところは、SPAMや嫌がらせの原因となる実メールアドレスの問題点を解決する通信網におけるメールアクセス制御方式を提供することにある。

【0027】本発明の他の目的は、ユーザの識別子を隠蔽しつつ、ユーザの身元を一意に特定可能にするメールアクセス制御方式を提供することにある。

【0028】

【課題を解決するための手段】本発明では、実メールアドレスの移転及び取り消しの問題を解決するために、個別化アクセスチケットを用いたメールアクセス制御方式を用いる。移転の問題を解決するためには、送信者の実メールアドレスと受信者の実メールアドレスの両者を含む個別化アクセスチケット（PAT: Personalized Access Ticket）を用いて宛先を指定する。また、取り消しの問題を解決するために、信頼できる第三者機関においてPATに有効期限を設定する。そして、有効期限を過ぎたPATを提示した送信者からのメールの配送を拒否する。また、実メールアドレスを取り消す代わりにPATをセキュア・コミュニケーション・サービスで管理するセキュアな記憶装置に登録する。

【0029】すなわち、本発明では送信者の実メールアドレスと受信者の実メールアドレスを対にした単位で接続を制御する。このため、実メールアドレスを移転されても、移転先のユーザによってPATを取得されない限り、移転先のユーザからのメールを受信しないで済む。

【0030】また、本発明では有効期限を過ぎたPAT、または受信者によってデータベースに登録されたPATを提示した送信者からのメールの配送をしないため、実メールアドレスを取り消すことなく受信を拒否できる。

【0031】また、本発明ではPATを前記記憶装置から削除することにより受信を再開するため、実メールアドレスを再取得することなく受信を再開できる。

【0032】また、本発明ではメールの送信をサーバ側で拒否するため、ユーザ側での受信やダウンロードに要する時間的、経済的負担を軽減できる。

【0033】さらに、本発明では、ユーザの匿名性を保証しつつ、ユーザの身元特定を可能にするために、個人識別子と役割識別子を用いたメールアクセス制御方式を用いる。

【0034】本発明では、ユーザを一意に特定するために、個人情報に信頼できる第三者機関の秘密鍵で署名した証明書を付与する。この証明書を以下では個人識別子（OID: Official Identification）と呼ぶ。また、ユーザの匿名性を保証しつつ身元特定を可能とするために、通信網上のユーザ識別子として個人識別子の情報を断片的に含む証明書を付与する。この証明書を以下では役割識別子（AID: Anonymous Identification）と呼ぶ。

【0035】また、本発明では、身元を特定するために、複数のAIDの同一性を判定しながらOIDを再構築する。AIDの移転および取り消しの問題を解決するために、AIDをPATに含め、セキュア・コミュニケーション・サービスSCSにおいてPATを検証する。

【0036】また、本発明では、身元を明らかにしないまま不特定多数からのアクセスを求めるユーザ側の需要に対して、AIDを不特定多数から検索可能なディレクトリで管理し、宛先としてAIDを含むPATを出力する。

【0037】これにより、本発明ではAIDはOIDを断片的にしか含まないため、メールの送受信において身元を隠蔽できる。また、AIDを不特定多数から閲覧可能なディレクトリサービスに登録しても、身元を不特定多数に対して隠蔽できる。

【0038】また、本発明では複数のAIDの同一性を判定しながらOIDを再構築することにより、確率的に身元を特定できる。このため、身元を明らかにしないSPAMや嫌がらせ行為への対策を立てることが可能である。

【0039】また、本発明では実メールアドレスの代わりにAIDをディレクトリで管理し、宛先としてAIDを含むPATを出力することにより、身元を明らかにしないまま不特定多数からのアクセスを受け付けることが可能である。

【0040】より詳細には、本発明は、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップと、を有することを特徴とするメールアクセス制御方法を提供する。

【0041】また、本発明では、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否することを特徴とする。

【0042】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証することを特徴とする。

【0043】また、本発明では、前記受け取るステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、前記制御するステップにおいて、該セキュア・コミュニケーション・サービスは発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否することを特徴とする。

【0044】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否することを特徴とする。

【0045】また、本発明では、前記個別化アクセスチケットの有効期限は信頼できる第三者機関により設定されたものであることを特徴とする。

【0046】また、本発明では、各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理するディレクトリ・サービスにおいて、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者に対して前記個別化アクセスチケットを発行するステップを、更に有することを特徴とする。

【0047】また、本発明では、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み、該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを、予め前記セキュア・コミュニケーション・サービスに登録するステップを更に有し、前記制御するステップにおいて、該セキュア・コミュニケーション・サービスは発信者により提示された個別化アクセスチケットがそこに予め登録されたものであるときには前記メールの配送を拒否することを特徴とする。

【0048】また、本発明では、前記登録するステップにおいて個別化アクセスチケットを登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービスにおいて登録された個別化アクセスチケットを削除するステップを、更に有することを特徴とする。

【0049】また、本発明では、前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービス

により発信者を認証すべきかどうかを示す移転制御フラグも含み、前記制御するステップにおいて、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、該セキュア・コミュニケーション・サービスは発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否することを特徴とする。

【0050】また、本発明では、前記発信者識別子の認証は、発信者と前記セキュア・コミュニケーション・サービス間のチャレンジ／レスポンス認証により実現することを特徴とする。

【0051】また、本発明では、前記個別化アクセスチケットの移転制御フラグは信頼できる第三者機関により設定されたものであることを特徴とする。

【0052】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の実メールアドレスにより与えられることを特徴とする。

【0053】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであることを特徴とする。

【0054】また、本発明では、前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【0055】また、本発明では、前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【0056】また、本発明では、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする。

【0057】また、本発明では、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられることを特徴とする。

【0058】また、本発明では、前記各役割識別子のリンク情報は、前記認証局により各役割識別子に一意に付与された識別子であることを特徴とする。

【0059】また、本発明では、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする。

【0060】また、本発明では、前記個別化アクセスチケットは、一つの発信者識別子と一つの着信者識別子を1対1に対応付けて含むことを特徴とする。

【0061】また、本発明では、前記個別化アクセスチケットは、一つの発信者識別子と複数の着信者識別子を1対N (Nは1より大きい整数) に対応付けて含むことを特徴とする。

【0062】また、本発明では、前記一つの発信者識別子と複数の着信者識別子の内の一識別子は前記個別化アクセスチケットの所有者を特定する所有者識別子であり、前記一つの発信者識別子と複数の着信者識別子の内の他の識別子は該所有者が属するグループの会員を特定する会員識別子であることを特徴とする。

【0063】また、本発明では、各ユーザの識別子と、各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnablerを認証局において各ユーザに発行して、該個別化アクセスチケットに含まれる所有者識別子と該所有者識別子に対応するEnablerの両方をセキュアな演算装置に対して提示したユーザによってのみ該セキュアな演算装置において該個別化アクセスチケットに対する所定の演算を行えるようにするステップを、更に有することを特徴とする。

【0064】また、本発明では、前記認証局は、それがEnablerであることを示す情報と各ユーザの識別子の実体に対し、該認証局の秘密鍵で署名したものを各ユーザの識別子のEnablerとして発行することを特徴とする。

【0065】また、本発明では、前記所定の演算は、個別化アクセスチケットの新規作成、複数個別化アクセスチケットのマージ、一個別化アクセスチケットの複数個別化アクセスチケットへの分割、個別化アクセスチケットの所有者変更、個別化アクセスチケットの有効期限の変更、個別化アクセスチケットの移転制御フラグの変更、を含むことを特徴とする。

【0066】また、本発明では、すべてのユーザに既知である特殊な識別子と該特殊な識別子に対応する特殊なEnablerを定義して、前記個別化アクセスチケットの新規生成および前記個別化アクセスチケットの所有者変更を、前記個別化アクセスチケットの所有者が、該特殊な識別子および該特殊なEnablerを用いて会員識別子のEnablerを使わずに行えるようにすることを特徴とする。

【0067】また、本発明では、前記特殊な識別子は、個別化アクセスチケットの所有者識別子としてのみ使用可能であるように定義されていることを特徴とする。

【0068】また、本発明では、すべてのユーザに既知である特殊な識別子を定義して、該特殊な識別子を用いて個別化アクセスチケットに読取専用属性を設定できるようにすることを特徴とする。

【0069】また、本発明では、前記制御するステップにおいて、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、前記セキュア・コミュニケーション・サービスは、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すことを特徴とする。

【0070】さらに、本発明は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義し、通信ネットワーク上のメールの通信において各ユーザを各ユーザの役割識別子により識別する、ことを特徴とするメールアクセス制御方法を提供する。

【0071】また、本発明では、前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【0072】また、本発明では、前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【0073】また、本発明では、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子と着信者の役割識別子に対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップ、を更に有することを特徴とする。

【0074】また、本発明では、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする。

【0075】また、本発明では、前記定義するステップは、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報も定義し、各役割識別子は各役割識

別子のリンク情報も含むことを特徴とする。

【0076】また、本発明では、前記各役割識別子のリンク情報は、前記認証局により各役割識別子に一意に付与された識別子であることを特徴とする。

【0077】また、本発明では、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップ、を更に有することを特徴とする。

【0078】また、本発明では、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする。

【0079】さらに、本発明は、複数のユーザ端末が接続された通信網と、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子に対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、該通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービス装置と、を有することを特徴とするメールアクセス制御を実現した通信システムを提供する。

【0080】また、本発明では、前記セキュア・コミュニケーション・サービス装置は発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否することを特徴とする。

【0081】また、本発明では、前記個別化アクセスチケットを自身の秘密鍵により署名して発行するセキュアな演算装置を更に有し、前記セキュア・コミュニケーション・サービス装置は該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証することを特徴とする。

【0082】また、本発明では、前記セキュア・コミュニケーション・サービス装置は発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれて

いるか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否することを特徴とする。

【0083】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記セキュア・コミュニケーション・サービス装置は発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否することを特徴とする。

【0084】また、本発明では、前記個別化アクセスチケットの有効期限を設定する信頼できる第三者機関を更に有することを特徴とする。

【0085】また、本発明では、各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者に対して前記個別化アクセスチケットを発行するディレクトリ・サービス装置を更に有することを特徴とする。

【0086】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み、該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを、予め登録し、発信者により提示された個別化アクセスチケットがそこに予め登録されたものであるときには前記メールの配送を拒否することを特徴とする。

【0087】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記個別化アクセスチケットを登録した前記特定の登録者からの要求により、そこに登録された個別化アクセスチケットを削除することを特徴とする。

【0088】また、本発明では、前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービス装置により発信者を認証すべきかどうかを示す移転制御フラグも含み、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、該セキュア・コミュニケーション・サービス装置は発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否することを特徴とする。

【0089】また、本発明では、前記発信者識別子の認証は、発信者と前記セキュア・コミュニケーション・サービス装置間のチャレンジ／レスポンス認証により実現することを特徴とする。

【0090】また、本発明では、前記個別化アクセスチ

ケットの移転制御フラグを設定する信頼できる第三者機関を更に有することを特徴とする。

【0091】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の実メールアドレスにより与えられることを特徴とする。

【0092】また、本発明では、それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子を発行する認証局装置を更に有し、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられることを特徴とする。

【0093】また、本発明では、前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする。

【0094】また、本発明では、前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする。

【0095】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする。

【0096】また、本発明では、それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とを発行する認証局装置を更に有し、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられることを特徴とする。

【0097】また、本発明では、前記各役割識別子のリンク情報は、前記認証局装置により各役割識別子に一意に付与された識別子であることを特徴とする。

【0098】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする。

【0099】また、本発明では、前記個別化アクセスチケットは、一つの発信者識別子と一つの着信者識別子を1対1に対応付けて含むことを特徴とする。

【0100】また、本発明では、前記個別化アクセスチ

ケットは、一つの発信者識別子と複数の着信者識別子を1対N (Nは1より大きい整数) に対応付けて含むことを特徴とする。

【0101】また、本発明では、前記一つの発信者識別子と複数の着信者識別子の内の一識別子は前記個別化アクセスチケットの所有者を特定する所有者識別子であり、前記一つの発信者識別子と複数の着信者識別子の内の他の識別子は該所有者が属するグループの会員を特定する会員識別子であることを特徴とする。

【0102】また、本発明では、各ユーザの識別子と、各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnablerを各ユーザに発行する認証局装置と、該個別化アクセスチケットに含まれる所有者識別子と該所有者識別子に対応するEnablerの両方を提示したユーザによってのみ該個別化アクセスチケットに対する所定の演算を行うことを可能としたセキュアな演算装置と、を更に有することを特徴とする。

【0103】また、本発明では、前記認証局装置は、それがEnablerであることを示す情報と各ユーザの識別子の実体に対し、該認証局の秘密鍵で署名したものを各ユーザの識別子のEnablerとして発行することを特徴とする。

【0104】また、本発明では、前記所定の演算は、個別化アクセスチケットの新規作成、複数個別化アクセスチケットのマージ、一個別化アクセスチケットの複数個別化アクセスチケットへの分割、個別化アクセスチケットの所有者変更、個別化アクセスチケットの有効期限の変更、個別化アクセスチケットの移転制御フラグの変更、を含むことを特徴とする。

【0105】また、本発明では、すべてのユーザに既知である特殊な識別子と該特殊な識別子に対応する特殊なEnablerを定義して、前記個別化アクセスチケットの新規生成および前記個別化アクセスチケットの所有者変更を、前記個別化アクセスチケットの所有者が、該特殊な識別子および該特殊なEnablerを用いて会員識別子のEnablerを使わずに行えるようにしたことを特徴とする。

【0106】また、本発明では、前記特殊な識別子は、個別化アクセスチケットの所有者識別子としてのみ使用可能であるように定義されていることを特徴とする。

【0107】また、本発明では、すべてのユーザに既知である特殊な識別子を定義して、該特殊な識別子を用いて個別化アクセスチケットに読取専用属性を設定できるようにしたことを特徴とする。

【0108】また、本発明では、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、前記セキュア・コミュニケーション・サービス装置は、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メ

ールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すことを特徴とする。

【0109】さらに、本発明は、それにより自身が各ユーザを一意的に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義する認証局装置と、そこでのメールの通信において各ユーザが各ユーザの役割識別子により識別される通信網と、を有することを特徴とするメールアクセス制御を実現した通信システムを提供する。

【0110】また、本発明では、前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする。

【0111】また、本発明では、前記各ユーザの個人識別子は、前記認証局により各ユーザに一意的に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【0112】また、本発明では、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子と着信者の役割識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、前記通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービス装置を更に有することを特徴とする。

【0113】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする。

【0114】また、本発明では、前記認証局装置は、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報も定義し、各役割識別子は各役割識別子のリンク情報も含むことを特徴とする。

【0115】また、本発明では、前記各役割識別子のリンク情報は、前記認証局装置により各役割識別子に一意的に付与された識別子であることを特徴とする。

【0116】また、本発明では、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス

権を検証することにより発信者と着信者間のアクセスを制御して、前記通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスを更に有することを特徴とする。

【0117】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする。

【0118】さらに、本発明は、コンピュータハードウェアと、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、発信者と着信者間の通信を接続するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュア・コミュニケーション・サービス装置を提供する。

【0119】また、本発明では、前記コンピュータソフトウェアは、発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【0120】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記コンピュータソフトウェアは、該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証するように前記コンピュータハードウェアを動作させることを特徴とする。

【0121】また、本発明では、前記コンピュータソフトウェアは、発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【0122】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記コンピュータソフトウェア

は、発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【0123】また、本発明では、前記コンピュータソフトウェアは、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め前記セキュア・コミュニケーション・サービスに登録し、発信者により提示された個別化アクセスチケットが前記セキュア・コミュニケーション・サービスに予め登録されたものであるときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【0124】また、本発明では、前記コンピュータソフトウェアは、個別化アクセスチケットを登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービスにおいて登録された個別化アクセスチケットを削除するように前記コンピュータハードウェアを動作させることを特徴とする。

【0125】また、本発明では、前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービスにより発信者を認証すべきかどうかを示す移転制御フラグも含み、前記コンピュータソフトウェアは、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【0126】また、本発明では、前記コンピュータソフトウェアは、前記発信者識別子の認証を、発信者と前記セキュア・コミュニケーション・サービス間のチャレンジ/レスポンス認証により実現するように前記コンピュータハードウェアを動作させることを特徴とする。

【0127】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであって、前記コンピュータソフトウェアは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータハードウェアを動作させることを特徴とする。

【0128】また、本発明では、それにより認証局が各

ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられ、前記コンピュータソフトウェアは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータハードウェアを動作させることを特徴とする。

【0129】また、本発明では、前記コンピュータソフトウェアは、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すように前記コンピュータハードウェアを動作させることを特徴とする。

【0130】さらに、本発明は、コンピュータハードウェアと、個別化アクセスチケットの要求をユーザから受け取り、発信者識別子と着信者識別子を対応付けて含み、自身の秘密鍵により署名された個別化アクセスチケットを発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置を提供する。

【0131】さらに、本発明は、コンピュータハードウェアと、各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者に対して、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるディレクトリ・サービス装置を提供する。

【0132】さらに、本発明は、コンピュータハードウェアと、それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を、各ユーザに対して発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システム

ムにおける認証局装置を提供する。

【0133】さらに、本発明は、コンピュータハードウェアと、各ユーザの識別子と、一般に一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの中で該各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnablerを各ユーザに対して発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおける認証局装置を提供する。

【0134】さらに、本発明は、コンピュータハードウェアと、一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの要求をユーザから受け取り、該ユーザが該個別化アクセスチケットに含まれる所有者識別子と該ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示し該所有者識別子に対応するEnablerの両方を提示したときに該個別化アクセスチケットに対する所定の演算を行うように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置を提供する。

【0135】さらに、本発明は、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子に対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、発信者と着信者間の通信を接続する、メールアクセス制御を実現した通信システムにおけるセキュア・コミュニケーション・サービス装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【0136】また、本発明では、前記プログラムは、発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【0137】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記プログラムは、該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証するように前記コンピュータを動作させることを特徴とする。

【0138】また、本発明では、前記プログラムは、発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【0139】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記プログラムは、発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【0140】また、本発明では、前記プログラムは、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め前記セキュア・コミュニケーション・サービス装置に登録し、発信者により提示された個別化アクセスチケットが前記セキュア・コミュニケーション・サービス装置に予め登録されたものであるときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【0141】また、本発明では、前記プログラムは、個別化アクセスチケットに登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービス装置において登録された個別化アクセスチケットを削除するように前記コンピュータを動作させることを特徴とする。

【0142】また、本発明では、前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービス装置により発信者を認証すべきかどうかを示す移転制御フラグも含み、前記プログラムは、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【0143】また、本発明では、前記プログラムは、前記発信者識別子の認証を、発信者と前記セキュア・コミュニケーション・サービス装置間のチャレンジ／レスポンス認証により実現するように前記コンピュータを動作させることを特徴とする。

【0144】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子

は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであって、前記プログラムは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータを動作させることを特徴とする。

【0145】また、本発明では、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられ、前記プログラムは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータを動作させることを特徴とする。

【0146】また、本発明では、前記プログラムは、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すように前記コンピュータを動作させることを特徴とする。

【0147】さらに、本発明は、個別化アクセスチケットの要求をユーザから受け取り、発信者識別子と着信者識別子に対応付けて含み、自身の秘密鍵により署名された個別化アクセスチケットを発行する、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【0148】さらに、本発明は、各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者に対して、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者識別子と着信者識別子に対応付けて含んだ個別化アクセスチケットを発行する、メールアクセス制御を実現した通信システムにおけるディレクトリ・サービス装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【0149】さらに、本発明は、それにより自身が各ユ

ーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を、各ユーザに対して発行する、メールアクセス制御を実現した通信システムにおける認証局装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【0150】さらに、本発明は、各ユーザの識別子と、一般に一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの中で各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnablerを各ユーザに対して発行する、メールアクセス制御を実現した通信システムにおける認証局装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【0151】さらに、本発明は、一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの要求をユーザから受け取り、該ユーザが該個別化アクセスチケットに含まれる所有者識別子と該ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示し該所有者識別子に対応するEnablerの両方を提示したときに該個別化アクセスチケットに対する所定の演算を行う、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【0152】

【発明の実施の形態】まず、図1乃至図7を参照して本発明の第1の実施形態について説明する。本発明のメールアクセス制御方法は、通信網における発信者および着信者の匿名性を保持しつつ、発信者と着信者間の双方向通信をも適宜可能とするものであり、基本的には着信者の本当の識別子を隠蔽した状態で、着信者の特性を表す情報のみを公開し、この公開された情報に基づいて、匿名性を保持したまま通信を希望する者に対して限定的なアクセス権を付与することにある。

【0153】具体的には、ユーザに対して個人情報を隠蔽した役割識別子(Anonymous Identification: AIDと略称する)を付与し、この役割識別子AIDをユーザの特性を表す情報である趣味、年齢、職業等のようなユーザをネットワーク上で特定はできないが、発信者にとって当該ユーザと通信する価値があるかどうかを判断するための有用な情報と組にしてネットワークに公開する。

【0154】また、発信者は、前記公開された情報を閲覧または検索することにより自分が通信したい相手を探すことができる。すなわち、発信者が発信者自身の匿名性を保持したままある相手と通信したい場合には、その相手の役割識別子を指定し、個別化アクセスチケットPAT(Personalized Access Ticket)を取得する。

【0155】個別化アクセスチケットPATには、発信者、着信者それぞれの役割識別子AIDの他に、移転制御フラグ、および、有効期限の各情報が記載されている。移転制御フラグは、セキュア・コミュニケーション・サービスSCS (Secure Communication Service) が送信者に対し認証を実行するか否かを決定するために使用される。すなわち、移転制御フラグを立てると、SCSは、接続要求の際に、発信者に対し、例えば署名の検証等の認証を行う。また、移転制御フラグを立てない場合には、セキュア・コミュニケーション・サービスSCSは認証無しで接続要求をセキュア・コミュニケーション・サービスSCSが接続している物理的通信網に渡す。すなわち、移転制御は役割識別子AIDがこれを認証局CA (Certification Authority) から割り当てられたユーザによって正当に利用されているかを認証するために用いられる。

【0156】本発明のメールアクセス制御方法を実施する通信網においては、ユーザに対する役割識別子AIDの付与、役割識別子AIDと組み合わされた公開情報の保持、個別化アクセスチケットPATの発行、および個別化アクセスチケットPATに基づくメールアクセス制御はそれぞれ別の機関で行われている。これは、それぞれの行為に関して保持すべきセキュリティレベルに差があるので、別々の機関で実行した方がネットワーク全体のセキュリティの保持には好都合だからである。但し、公開情報の保持とPATの発行は同一の機関で行ってもよい。

【0157】図1は、本第1の実施形態の通信システムの全体構成図である。本実施形態はインターネットまたはイントラネット上の電子メールサービスを対象としたものである。図1において、1は認証局CAであり、個人識別子OIDの認証権限と役割識別子AIDの発行権限を有し、個人識別子OIDから役割識別子AIDを生成し、ユーザに対して役割識別子AIDを割り当てる機能を有する。3はユーザである。5はセキュア・コミュニケーション・サービスSCSであり、ユーザ3からの電子メールによる接続要求に対し接続を許可するか否かを、ユーザ3から提示された個別化アクセスチケットを用いて判定する。また、ユーザ3からの要求に基づいて、電子メールによる接続要求を拒否する。また、ユーザ3からの要求に基づいて、個人識別子OIDの同一性を判定する。7はアノニマス・ディレクトリ・サービスADSであり、役割識別子AID、移転制御フラグの値、有効期限の値、及び、ユーザ3についての公開情報（趣味等、氏名、電話番号、実Eメールアドレス等の個人情報に比べ秘密性の低いと考えられる情報）を管理するデータベースである。アノニマス・ディレクトリ・サービスADS7は、検索条件を提示したユーザ3の役割識別子AID、検索条件を満足する公開情報をアノニマス・ディレクトリ・サービスADS7に登録していたユ

ーザ3の役割識別子AID、ユーザ3または管理者等により与えられた移転制御フラグの値、及び、ユーザ3または管理者等により与えられた有効期限の値から個別化アクセスチケットPATを生成し、検索条件を提示したユーザ3に割り当てる機能を有する。

【0158】まず、ユーザの要求に基づいて個人識別子から役割識別子AIDを生成し、そのユーザに割り当てるまでの一連の処理について説明する。

【0159】図2は、個人識別子OID、役割識別子AIDおよび個別化アクセスチケットPATの例を示している。個人識別子OIDは、図2(a)に示すように、認証局CA1がユーザを一意的に識別可能な規則に従う任意の文字列と公開鍵から構成される情報に対し、認証局CA1が署名したものである。また、役割識別子AIDは、図2(b)に示すように、個人識別子OIDの断片とその位置情報、冗長な文字列、SCSを動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列（ホスト名、実ドメイン名等）であるSCSの情報から構成される情報に対し、認証局CA1が署名したものである。

【0160】また、個別化アクセスチケットPATは、図2(c)に示すように、移転制御フラグ、役割識別子AID₀、役割識別子AID₁、有効期限から構成される情報に対して、アノニマス・ディレクトリ・サービスADSが署名したものである。ここで、移転制御フラグの値は、0または1のいずれかであると定義する。また、有効期限はPATの使用回数、PATが利用不可能になる絶対時刻(UTC)、PATが利用可能になる絶対時刻(UTC)、PATが利用可能になってから利用不可能になるまでの相対時間(寿命)のいずれか、または複数を組み合わせて定義する。

【0161】更に、後述する各実施形態で説明するように、本発明は、個別化アクセスチケットPATとして、上述した1対1個別化アクセスチケットに加えて、発信者と着信者を1対Nに対応させている1対N個別化アクセスチケット、および役割識別子の実体を個別化アクセスチケットで指定する代わりに役割識別子を指定するリンク情報を持ち、このリンク情報で役割識別子を指定するリンク指定型個別化アクセスチケットを有し、このリンク指定型個別化アクセスチケットには上述した発信者と着信者の対応関係に基づきリンク指定型1対1個別化アクセスチケットとリンク指定型1対N個別化アクセスチケットがある。すなわち、本発明の個別化アクセスチケットには、1対1個別化アクセスチケット、1対N個別化アクセスチケット、リンク指定型1対1個別化アクセスチケット、およびリンク指定型1対N個別化アクセスチケットの4種類がある。

【0162】次に、ユーザ3が役割識別子AIDを認証局CA1に対して要求する手続きについて説明する。ユーザ3は秘密鍵と公開鍵のペアを生成する。次に、ユー

ザ3の個人識別子OIDと認証局CA1の証明書を用いて、ユーザ3と認証局CA1との間で双方向認証を行う。次に、ユーザ3は該公開鍵を認証局CA1に任意の手段で送信する。

【0163】なお、上記手続きにおいて、ユーザ3と認証局CA1間の通信を暗号化する場合もある。

【0164】次に、上述した役割識別子AIDの要求に対し、認証局CA1が役割識別子AIDをユーザ3に対して交付する手続きについて説明する。認証局CA1は、ユーザ3からの公開鍵を受信すると、役割識別子AIDを生成する。次に、認証局CA1は該役割識別子AIDをユーザ3に任意の手段で送信する。ユーザ3は認証局CA1から役割識別子AIDを受信すると、受信した該役割識別子をユーザ3の記憶装置に記録する。

【0165】なお、上記手続きにおいて、ユーザ3と認証局CA1間の通信を暗号化する場合もある。

【0166】次に、認証局CA1における役割識別子AIDの生成処理について図3に示すフローチャートを用いて説明する。図3において、認証局CA1は個人識別子OIDの全長Lと等しい長さの情報を生成する。この情報を仮の役割識別子AIDとする（ステップS911）。次に、OIDの部分複写を行うために、OIDの複写範囲を指定するパラメータ p_i と l_i の値をそれぞれ乱数発生等の任意の手段を用いて決定する（ステップS913）。ここで、Lは個人識別子OIDの全長と等しく、 l_i は $0 \leq p_i \leq L$ の関係が成立する範囲で任意に定めた値とする。次に、OIDの先頭から位置 p_i から位置 $p_i + l_i$ の範囲の情報を、仮AIDの同じ位置に複写する（ステップS915）。つまり、このOID断片は仮AIDの先頭から位置 p_i と位置 $p_i + l_i$ の範囲に複写される。次に、OIDを部分複写した仮AIDの定められた範囲に、 p_i と l_i の値を任意の手段で暗号化して書き込む（ステップS917）。次に、これらの値を書き込んだ仮AIDの定められた範囲にセキュア・コミュニケーション・サービスSCS5を動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列（ホスト名、実ドメイン等）であるSCSの情報を書き込む（ステップS919）。次に、文字列を書き込んだ仮AIDに認証局CA1の秘密鍵で署名する（ステップS921）。

【0167】次に、ユーザB3の役割識別子AID及び公開情報をアノニマス・ディレクトリ・サービスADS7に登録する手続きについて説明する。登録者であるユーザB3とアノニマス・ディレクトリ・サービスADS7との間で、ユーザB3の役割識別子AIDとADS7の証明書を用いて、任意の手段で双方向認証を行う。次に、ユーザB3は、移転制御フラグの値、有効期限の値、および、趣味等の公開情報をADS7に送信する。次に、ADS7はユーザB3から受信した移転制御フラグの値、有効期限の値、すべての公開情報を、すべてユ

ーザB3のAIDと関連付けて記憶装置に記録する。

【0168】なお、上記手続きにおいて、登録者であるユーザB3とADS7間の通信を暗号化する場合もある。

【0169】次に、ユーザA3がアノニマス・ディレクトリ・サービスADS7に登録された公開情報を検索する手続きについて説明する。検索者であるユーザA3とアノニマス・ディレクトリ・サービスADS7との間で、ユーザA3の役割識別子AIDとADS7の証明書を用いて、任意の手段で双方向認証を行う。次にユーザA3は任意の検索条件をADS7に送信する。次に、ADS7は受信したすべての検索条件を記憶装置に提示し、これらの検索条件を満足する登録者の役割識別子AIDを抽出する。次に、ADS7はユーザA3のAIDと検索条件を満足した登録者のAIDと移転制御フラグの値と有効期限の値から個別化アクセスチケットPATを生成する。次に、ADS7は生成したPATをユーザA3に送信する。

【0170】なお、上記手続きにおいて、検索者であるユーザA3とADS7間の通信を暗号化する場合もある。

【0171】1対1個別化アクセスチケットは、アノニマス・ディレクトリ・サービスADS7の検索結果として生成する。

【0172】次に、図4に示すフローチャートを参照して、ADSにおける1対1個別化アクセスチケットPATの生成処理について説明する。まず、ある定められた長さの情報を生成する。これを仮の個別化アクセスチケット（仮PAT）とする（ステップS1210）。次に、検索者であるユーザA3の役割識別子AIDと登録者であるユーザB3の役割識別子AIDを仮PATの定められた範囲に複写する（ステップS1215）。次に、移転制御フラグの値と有効期限の値をそれぞれ、AIDを複写した仮PATの定められた範囲に書き込む（ステップS1217）。次に、これらの値を書き込んだ仮PATにADSの秘密鍵で署名する（ステップS1219）。

【0173】次に、1対1個別化アクセスチケットPATによる移転制御について説明する。移転制御とは、PATを譲渡されたあるいは盗聴した第三者（本来はアクセス権を有していないユーザ）から、正当なアクセス権を持つユーザへのアクセスを制限する機能である。

【0174】アノニマス・ディレクトリ・サービスADS7および登録者AIDのユーザB3は、個別化アクセスチケットPATの移転制御フラグにある値を設定することにより、アクセス権を有していない第三者からのユーザB3への接続を禁止することができる。

【0175】移転制御フラグの値を1に設定した場合には、セキュア・コミュニケーション・サービスSCS5と発信者との間で任意のチャレンジ/レスポンス方式に

従い発信者役割識別子AIDを認証するため、発信者が発信者AIDとPATの両者を発信者以外のいかなるユーザに渡しても、そのユーザは登録者にSCS5を介して接続できない。

【0176】一方、移転制御フラグの値を0に設定した場合には、SCS5と発信者との間でいかなるチャレンジ/レスポンスも行わないため、発信者が発信者AIDとPATの両者を発信者以外のユーザに渡したら、それらのユーザもアノニマス・ディレクトリ・サービスの登録者とSCS5を介して接続できるようになる。

【0177】次に、図5を参照してSCSにおけるメールアクセス制御方法について説明する。

【0178】発信者はFrom:行に"発信者AID@発信者のSCSの実ドメイン"、To:行に"PAT@発信者のSCSの実ドメイン"の形式で指定する。

【0179】SCSはSMTP(Simple Mail Transfer Protocol)等のMTA(Message Transfer Agent)の受信したメールを取得し、図5に示す処理を実行する。

【0180】1. PATの署名をADS7の公開鍵を用いて検証する(ステップS1413)。

【0181】・PATに改竄が認められる場合(ステップS1415YES)、メールを廃棄して終了する(ステップS1416)。

【0182】・PATに改竄が認められ得ない場合(ステップS1415NO)、下記処理2.を実行する。

【0183】2. 発信者AIDをPATに提示して検索する(ステップS1417、S1419、S1421)。

【0184】・発信者AIDと完全一致するAIDがPATに含まれていない場合には(ステップS1423NO)、メールを廃棄して終了する(ステップS1416)。

【0185】・発信者AIDと完全一致するAIDがPATに含まれている場合には(ステップS1423YES)、下記処理3.を実行する。

【0186】3. PATの有効期限の値を評価する(ステップS1425、S1427)。

【0187】・PATが有効期限外の場合には(ステップS1427NO)、メールを廃棄して終了する(ステップS1416)。

【0188】・PATが有効期限内の場合には(ステップS1427YES)、下記処理4.を実行する。

【0189】4. PATの移転制御フラグの値を参照して、発信者を認証するか否かを決定する(ステップS1431、S1433)。

【0190】・値が1の場合には(ステップS1433YES)、SCSと発信者との間でチャレンジ/レスポンス認証を実行し、発信者の署名を検証する(ステップS1435)。署名が正しい場合には、着信者を指定し、PATを添付する(ステップS1437)。署名が

正しくない場合には、メールを廃棄して終了する(ステップS1416)。

【0191】・値が0の場合には(ステップS1433NO)、チャレンジ/レスポンス認証を実行せずに、着信者を指定し、PATを添付する(ステップS1437)。

【0192】次に、SCSと発信者との間のチャレンジ/レスポンスの例を説明する。まず、SCSは任意の情報、例えばタイムスタンプを生成し、生成した情報を発信者に送信する。

【0193】次に、発信者は、受信した情報に発信者AIDの秘密鍵で署名し、発信者AIDの公開鍵とあわせてSCSに送信する。

【0194】SCSは、受信した情報の署名を発信者AIDの公開鍵を用いて検証する。署名が正しい場合には、着信者を指定し、PATを添付する。署名が正しくない場合にはメールを廃棄して終了する。

【0195】次に、SCSにおける着信者の指定方法について説明する。SCSは、まず、発信者AIDをPATに提示して検索し、発信者AIDと完全一致しないすべてのAIDを取得する。取得したすべてのAIDを以後、着信者AIDと定義する。次に、すべての着信者AIDについて、それぞれ、着信者AIDから着信者のSCSの実ドメインを取り出す。次に、着信者を"着信者AID@着信者のSCSの実ドメイン"の形式で指定する。最後に、SCSは発信者を"発信者AID@発信者のSCSの実ドメイン"の形式から"発信者AID"の形式に変更する。

【0196】次に、SCSにおけるPATの添付方法について説明する。SCSは、PATをメールの任意の箇所に添付する。

【0197】発信者及び受信者を指定しPATを添付してから、SCSは、MTAにメールを渡す。

【0198】なお、上記すべての処理は、1対N個別化アクセスチケットの場合も同様である。

【0199】次に、SCSにおける個別化アクセスチケットPATに対する着信拒否方法について説明する。

【0200】着信拒否の設定：ユーザとセキュア・コミュニケーション・サービスSCS5との間で、任意の手段で双方向認証を行う。次に、ユーザは登録命令とユーザ自身のAIDと任意のPATをSCS5に送信する。次に、SCS5は受信したAIDの署名を検証する。署名が正しくない場合には、SCS5は処理を終了する。署名が正しい場合には、SCS5は受信したすべてのPATについて、それぞれADSの公開鍵を用いて署名を検証する。署名が正しくないPATについては廃棄する。署名が正しい場合には、受信したAIDをそれぞれのPATに提示して検索する。受信したAIDと完全一致するAIDを含むPATについては、登録命令とPATを記憶装置に提示して、PATを記憶装置に登録す

る。受信したAIDと完全一致するAIDを含まないPATについては記憶装置に登録せずに廃棄する。なお、上記処理において、ユーザとSCS5間の通信を暗号化する場合もある。

【0201】着信拒否の実行：SCS5はPATを記憶装置に提示して検索する。提示したPATと完全一致するPATが記憶装置に登録されている場合には、メールを廃棄する。提示したPATと完全一致するPATが記憶装置に登録されていない場合には、メールを廃棄しない。

【0202】着信拒否の解除：ユーザとセキュア・コミュニケーション・サービスSCS5との間で、任意の手段で双方向認証を行う。次に、ユーザは自らのAIDをSCS5に提示する。次に、SCS5は受信したAIDの署名を検証する。署名が正しくない場合には、SCS5は処理を終了する。署名が正しい場合には、SCS5は提示されたAIDを検索条件として記憶装置に提示して、提示されたAIDを含むすべてのPATを取得し、ユーザに提示する。次に、ユーザは提示されたすべてのPATを参照し、着信拒否を解除したいPATをすべて選択し、削除命令と併せてSCS5に送信する。削除命令と着信拒否を解除したいすべてのPATを受信したSCS5は、受信した削除命令及びすべてのPATを記憶装置に提示して、受信したすべてのPATを記憶装置から削除する。

【0203】なお、SCSにおける1対N個別化アクセスチケットPATに対する着信拒否方法も、上記1対1個別化アクセスチケットに対する着信拒否方法と同様である。

【0204】また、ユーザBからユーザAへのメールの返信は、ユーザAからユーザBへのメールの送信の場合と同様である。

【0205】次に、図6のフローチャート及び図7を参照して、同一性の判定について説明する。

【0206】1. 変数OID_Mの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する。また、変数OID_Vの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する（ステップS2511）。

【0207】2. 処理対象のAIDの集合から1個のAIDを選択し、以下のビット演算を実行する（ステップS2513）。

【0208】(a) AIDに含まれる位置情報をもとにして、変数AID_Mと変数AID_Vの値を決定する（ステップS2515）。ここで、

- ・AID_MはOIDの全長Lと等しい長さで、かつ、
- －OID情報が定義されている位置の値は1である。
- －OID情報が定義されていない位置の値は0である。

- ・AID_VはOIDの全長Lと等しい長さで、かつ、

- －OID情報が定義されている位置の値はOID情報の実際の値である。

- －OID情報が定義されていない位置の値は0である。

ビット列と定義する（図7）。

【0209】(b) OID_MとAID_MのAND演算を実行し、その結果を変数OVR_Mに代入する（ステップS2517）。

【0210】(c) OVR_MとAID_MのAND演算と、OVR_MとOID_MのAND演算を実行し、その演算結果を比較する（ステップS2519）。

【0211】・一致する場合OID_MとAID_MのOR演算を実行し、実行結果をOID_Mに代入する（ステップS2521）。また、OID_VとAID_VのOR演算を実行し、実行結果をOID_Mに代入する（ステップS2523）。

【0212】・一致しない場合、ステップS2525に進み、実行する。

【0213】(d) 処理対象のAIDの集合から、次に処理するAIDを抽出する。

【0214】・集合に少なくとも1個のAIDが含まれている場合、ステップS2513～S2523を実行する。

【0215】・集合にAIDが1個も含まれていない場合、ステップS2527に進む。

【0216】(e) OID_MおよびOID_Vの値を出力する（ステップS2527）。

【0217】最終的に得られたOID_Mの値は、処理対象のAIDの集合から復元できたOID情報のすべての位置を表している。また、最終的に得られたOID_Vの値は、処理対象のAIDの集合から復元できたOID情報のすべてを表している。つまり、OID_MとOID_Vの値を用いると、

(a) OID_Vの値を検索条件とすると、確率的にはあるがOIDを求めることができる。

【0218】(b) 上記検索の精度を、OID全長Lとの比OID_M/Lで定量的に評価することができる。

【0219】上述したように、本実施形態では、ユーザ要求に基づいて、秘密性且つ信用性の高い第三者機関である認証局CA1において、氏名、電話番号、実Eメールアドレス等秘密性の高い個人情報を含む個人識別子AIDからこれらの個人情報を隠蔽した役割識別子AIDを生成し、ユーザに交付する。このAIDを用いて通信網及び通信網上で提供される各種サービスにおいてユーザを識別することにより、ユーザの匿名性保証と本人保証の両立が可能になる。つまり、ユーザは実名や電話番号やEメールアドレスを相手に教えずとも、お互いに通信できるようになるし、後述のようにアノニマス・ディレクトリ・サービスADS7を介して不特定多数に公開情報を開示することもできる。

【0220】ユーザは、個人情報に比べ秘密性のより低

いと思われる情報すなわち公開情報をアノニマス・ディレクトリ・サービスADS7に登録する。公開情報及び登録者AIDを検索する場合には、検索者は検索者の役割識別子AIDと任意の検索条件をADS7に提示する。ADS7はすべての検索条件を満足する登録者の役割識別子AIDを抽出し、次に、検索者AIDと検索条件を満足した登録者のAIDと移転制御フラグの値と有効期限の値から個別化アクセスチケットPATを生成する。

【0221】この1対1個別化アクセスチケットPATには、図2(c)に示すように移転制御フラグの値、有効期限の値が設定されるが、この有効期限を事前に設定することにより、発信者からの接続を制限することができる。

【0222】また、移転制御フラグの値により、アクセス権を有していない第三者からの接続を禁止することができる。すなわち、移転制御フラグの値を1に設定した場合には、セキュア・コミュニケーション・サービスSCS5と発信者との間で任意のチャレンジ/レスポンス方式に従い発信者役割識別子AIDを認証するため、発信者が発信者AIDとPATの両者を発信者以外のいかなるユーザに渡しても、そのユーザはアノニマス・ディレクトリ・サービスADS7への登録者にSCS5を介して接続できない。一方、移転制御フラグの値を0に設定した場合には、SCS5と発信者との間でいかなるチャレンジ/レスポンスも行わないため、発信者が発信者AIDとPATの両者を発信者以外のユーザに渡したら、それらのユーザもADS7への登録者にSCS5を介して接続できるようになる。

【0223】また、1対1個別化アクセスチケットPATで着信者を指定した呼を個別化アクセスチケットPAT内で定義した着信者役割識別子AIDまたは発信者役割識別子AIDに着信するように、通信網に対して接続要求をすることができる。更に、1対1個別化アクセスチケットPATで指定した呼のうち、着信者が選択した1対1個別化アクセスチケットPATの呼を着信拒否することができる。また、着信者が選択した1対1個別化アクセスチケットの呼の着信拒否を解除することもできる。更に、匿名性を悪用し複数の発信者役割識別子AIDで個人攻撃を繰り返す発信者への対処として、それら複数の発信者役割識別子AIDから個人識別子OIDの同一性を判定することができ、かつ、その個人識別子がある確率で取り出すことができる。

【0224】次に、本発明の第2の実施形態に係るメールアクセス制御方法について図8乃至図24を参照して説明する。上述した第1の実施形態では発信者と着信者を1対1に対応させる場合について説明したのに対して、第2の実施形態では、発信者と着信者を1対Nに対応させるとともに、この1対N個別化アクセスチケットの新規生成、内容変更をユーザ主導で可能とする場合に

ついて説明するものである。なお、この発信者はPATの所有者またはPATの会員のいずれかである。同様に受信者もPATの所有者またはPATの会員のいずれかである。

【0225】一般に、グループ通信（メーリングリスト等）の会員構成は動的に変化するため、グループ通信の主催者は会員の電話番号、Eメールアドレス等の連絡先情報を管理する必要がある。これに対して、第1の実施形態のように、1対1個別化アクセスチケットの新規生成しかできない場合には、連絡先情報の管理が困難である。例えば、グループを一体として管理することが困難であり、また移転制御のため、他の人に渡しても、メーリングリスト等グループ通信のアドレスとして機能しない。

【0226】本第2の実施形態では、このような不具合を解消するために1対N個別化アクセスチケットPATの新規生成および既存の1対N個別化アクセスチケットPATの内容変更をユーザ主導でできるようにしている。

【0227】まず、本第2の実施形態で使用される各識別子の定義について図8、図9を参照して説明する。

【0228】個人識別子(Official Identification: OID)は、図8(a)に示すように、認証局(Certificate Authority: CA)がユーザを一意に認識可能な規則に従う任意の文字列（電話番号、電子メールアドレス等）と公開鍵から構成される情報に対し、認証局CAが署名したものである。

【0229】役割識別子(Anonymous Identification: AID)は、図8(b)に示すように、個人識別子OIDの断片とその位置情報、冗長な文字列、SCSを動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列（ホスト名、実ドメイン名等）であるSCSの情報から構成される情報に対し、認証局CAが署名したものである。

【0230】1対N個別化アクセスチケットPATは、図8(c)に示すように、2個以上の役割識別子、所有者インデックス、有効期限、移転制御フラグ、PAT演算装置識別子から構成される情報に対し、PAT演算装置の秘密鍵で署名したものである。

【0231】ここで、役割識別子AIDの1個はこのPATの所有者役割識別子AIDで、所有者AIDとこれに対応したEnablerをPAT演算装置に提示することにより、PATへのAIDの追加、PATからのAIDの削除、PATの有効期限の変更、PATの移転制御フラグの値の変更等、PATに含まれる情報を変更することができる。

【0232】一方、PATに含まれる所有者AID以外のAIDはすべて会員AIDで、会員AIDとこれに対応したEnablerをPAT演算装置に提示しても、PATに含まれる情報を変更することはできない。

【0233】所有者インデックスは、所有者AIDを識別するための数値データで、所有者AIDと会員AIDから構成されるAIDリストにおける先頭のAIDが所有者AIDの場合には1、先頭から2番目のAIDが所有者AIDの場合には2、…、n番目の場合にはnであると定義する。移転制御フラグは、1対1個別化アクセスチケットの場合と同様、0または1の値をとりうると定義する。

【0234】所有者AIDは、AIDリストにおける所有者インデックスの値の位置に書き込まれているAIDであると定義する。会員AIDは、所有者AID以外のすべてのAIDと定義する。有効期限は、PATの使用回数、PATが利用不可能になる絶対時刻(UTC)、PATが利用可能になる絶対時刻(UTC)、PATが利用可能になってから利用不可能になるまでの相対時間(寿命)のいずれか、または複数を組み合わせて定義する。PAT演算装置(またはネットワーク上のPAT演算オブジェクト)の識別子は、PAT演算装置のシリアルナンバー(またはPAT演算オブジェクトのネットワーク上の識別名)であると定義する。PAT演算装置(またはネットワーク上のPAT演算オブジェクト)の秘密鍵は、前記識別子に一意に対応すると定義する。

【0235】また、本第2の実施形態では、役割識別子AIDに対応した識別子として、Enablerを導入している。Enablerは、図9に示すように、Enablerであることを一意に表す文字列とAIDから構成される情報に対して、認証局CA1が署名したものである。

$$\begin{aligned} & AID_A + AID_B + \text{Enabler of } AID_B + \text{Enabler of } AID_A \\ & \rightarrow ALIST < AID_A | AID_B > \\ & ALIST < AID_A | AID_B > + \text{Enabler of } AID_A \\ & + \text{有効期限の値} + \text{移転制御フラグの値} \\ & \rightarrow PAT < AID_A | AID_B > \end{aligned}$$

(2) マージ (MergePAT) (図11参照) :

同一所有者AIDの複数ALISTをマージし、マージ後のALISTに対し、有効期限の値および移転制御フ

【0236】次にPATの新規生成および内容変更における操作について説明する。通信端末上のセキュアPAT演算装置、CA上もしくはCAから正当に依頼されたネットワーク上のPAT演算オブジェクト(以後、これもPAT演算装置と呼ぶことにする)において、次の操作が定義される。

【0237】1. AIDリストの編集

AIDとEnablerを用いて、PATに含まれるAIDのリスト(以後、AIDリストと呼ぶ)を編集する。または、AIDリストを新規生成する。

【0238】2. 有効期限および移転制御フラグの設定
AIDとEnablerを用いて、PATに含まれる有効期限の値及び移転制御フラグの値を変更する。または、新たに生成したAIDリストに新たな有効期限の値及び新たな移転制御フラグの値を設定する。

【0239】所有者AIDとこの所有者AIDに対応したEnablerをPAT演算装置に提示したユーザは、PATに含まれるAIDのリストを編集できる。このとき、以下の演算規則に従う。

【0240】(1) 新規生成 (MakePAT) (図10参照) :

AIDリスト (ALIST < 所有者AID | 会員AID₁, 会員AID₂, ..., 会員AID_n >) を新規生成し、生成後のALISTに対し、有効期限の値および移転制御フラグの値を設定する。

【0241】

【数1】

ラグの値を設定する。

【0242】

【数2】

$$\begin{aligned} & ALIST < AID_A | AID_{B1}, AID_{B2}, \dots > \\ & + ALIST < AID_A | AID_{C1}, AID_{C2}, \dots > \\ & + \text{Enabler of } AID_A \\ & \rightarrow ALIST < AID_A | AID_{B1}, AID_{B2}, \dots, \\ & \quad AID_{C1}, AID_{C2}, \dots > \\ & ALIST < AID_A | AID_{B1}, AID_{B2}, \dots, AID_{C1}, AID_{C2}, \dots > \\ & + \text{Enabler of } AID_A + \text{有効期限の値} + \text{移転制御フラグの値} \\ & \rightarrow PAT < AID_A | AID_{B1}, AID_{B2}, \dots, AID_{C1}, AID_{C2}, \dots > \end{aligned}$$

(3) 分割 (SplitPAT) (図12参照) :

ALISTを同一所有者AIDの複数ALISTに分解し、分解後のすべてのALISTに対し、それぞれ、有

効期限の値および移転制御フラグの値を設定する。

【0243】

【数3】

$$\begin{aligned} & ALIST < AID_A | AID_{B1}, AID_{B2}, \dots, \\ & \quad AID_{C1}, AID_{C2}, \dots > + \text{Enabler of } AID_A \\ & \rightarrow ALIST < AID_A | AID_{B1}, AID_{B2}, \dots > \\ & + ALIST < AID_A | AID_{C1}, AID_{C2}, \dots > \end{aligned}$$

ALIST<AID_A | AID_{C1}, AID_{C2}, ...>
 + Enabler of AID_A + 有効期限の値 + 移転制御フラグの値
 → PAT<AID_A | AID_{C1}, AID_{C2}, ...>

(4) 所有者変更 (TransPAT) (図13参照) : する。
 ALISTの所有者AIDを変更し、変更後のALIS 【0244】
 Tに対し有効期限の値および移転制御フラグの値を設定 【数4】

ALIST<AID_A | AID_B>
 + ALIST<AID_A | AID_{C1}, AID_{C2}, ...>
 + Enabler of AID_A + Enabler of AID_B
 → ALIST<AID_B | AID_{C1}, AID_{C2}, ...>
 ALIST<AID_B | AID_{C1}, AID_{C2}, ...>
 + Enabler of AID_B + 有効期限の値 + 移転制御フラグの値
 → PAT<AID_B | AID_{C1}, AID_{C2}, ...>

有効期限の値の設定における操作では、所有者AIDと 義する。
 これに対応したEnabler の両者を所有するユーザにのみ 【0245】
 有効期限の値の設定を許可するために、以下の操作を定 【数5】

PAT<AID_A | AID_B> + Enabler of AID_A + 有効期限の値
 → PAT<AID_A | AID_B>

移転制御フラグの値の設定における操作では、所有者A 下の操作を定義する。
 IDとこれに対応したEnabler の両者を所有するユーザ 【0246】
 にのみ移転制御フラグの値の設定を許可するために、以 【数6】

PAT<AID_A | AID_B> + Enabler of AID_A
 + 移転制御フラグの値
 → PAT<AID_A | AID_B>

次に、本実施形態の全体構成を示す図14～図20につ
 いて説明する。図14～図20において、CAからAID_A
 を割り当てられたユーザAは、ユーザAの計算機に
 AID_A および Enabler of AID_A を保存し、フロッ
 ピードライブ、CD-ROMドライブ、通信ボード、マ
 イクロフォン、スピーカー等の入出力機器を接続してい
 る。または、記憶装置及びデータ入出力機能を備える通
 信端末 (電話、携帯電話等) に、AID_A および Enab
 ler of AID_A を保存している。

【0247】同様に、CAからAID_B を割り当てられ
 たユーザBは、自らの計算機にAID_B および Enabler
 of AID_B を保存し、フロッピードライブ、CD-R
 OMドライブ、通信ボード、マイクロフォン、スピーカ
 ー等の入出力機器を接続している。または、記憶装置及
 びデータ入出力機能を備える通信端末 (電話、携帯電話
 等) に、AID_B および Enabler of AID_B を保存し
 ている。

【0248】以下、ユーザAがPAT<AID_A | AID_B>
 を生成する手順を説明する。

(1) ユーザAは、以下の手段のいずれかを用いて、AID_B
 および Enabler of AID_B を取得する。

【0249】・アノニマス・ディレクトリ・サービスA
 DS7にAID_B と Enabler of AID_B を登録し、ユー
 ザAが検索結果として取得するのを待つ (図14)。

【0250】・電子メール、シグナリング等でAID_B
 と Enabler of AID_B をユーザAに直接送信する (図

15～図16)。

【0251】・フロッピーディスク、CD-ROM、M
 O、ICカード等の磁気、光、電子メディアにAID_B
 と Enabler of AID_B を蓄積し、ユーザAに渡す。ま
 たは、ユーザAが閲覧して取得するのを待つ (図17～
 図18)。

【0252】・書籍、名刺等の紙メディアにAID_B と
 Enabler of AID_B を記載し、ユーザAに渡す。もし
 くは、ユーザAが閲覧し取得するのを待つ (図19～図
 20)。

【0253】(2) 上述した(1)のいずれかの手段でA
 ID_B および Enabler of AID_B を取得したユーザA
 は、PAT演算装置に対しMakePAT命令を発行する。
 この手順は図14～図20で共通で、以下の通りに定義
 する。

【0254】(a) ユーザAは、ユーザAの通信端末にA
 ID_A、Enabler of AID_A、AID_B、Enabler o
 f AID_B、有効期限の値、および移転制御フラグの値
 をセットし、MakePAT命令の発行を要求する。

【0255】(b) ユーザAの通信端末は、MakePAT命
 令を生成する。

【0256】(c) ユーザAの通信端末は、生成したMake
 PAT命令を電子メール、シグナリング等の手段でPA
 T演算装置に送信する (MakePAT命令の発行)。

【0257】(d) PAT演算装置は、受信したMakePA
 T命令を図21、図23に従って処理し、PAT<AI

$D_A \mid AID_B >$ を生成する。具体的には、

【数7】

$$\begin{aligned} & AID_A + AID_B + \text{Enabler of } AID_B + \text{Enabler of } AID_A \\ & \rightarrow ALIST < AID_A \mid AID_B > \\ & ALIST < AID_A \mid AID_B > + \text{Enabler of } AID_A \\ & + \text{有効期限の値} + \text{移転制御フラグの値} \\ & \rightarrow PAT < AID_A \mid AID_B > \end{aligned}$$

(e) PAT演算装置は、生成した $PAT < AID_A \mid AID_B >$ を電子メール、シグナリング等の手段でユーザAの通信端末、または必要に応じて、ユーザBの通信端末に送信する。

【0258】(f) ユーザA（またはユーザB）の通信端末は、受信した $PAT < AID_A \mid AID_B >$ をユーザAの通信端末の記憶装置に保存する。

【0259】PATのマージ(MergePAT、図21、図23)、PATの分割(SplitPAT、図22、図23)、PATの所有者変更(TransPAT、図21、図23)も同様の手順である。

【0260】次に、図21のフローチャートを参照して、MakePAT、MergePAT、TransPATの手順について説明する。

【0261】1. 所有者AIDを指定する(ステップS4411)。

【0262】2. 会員AIDをすべて指定する(ステップS4412)。

【0263】3. 指定した所有者AIDと指定したすべての会員AIDからAIDリストを生成する(ステップS4413)。具体的には、任意の手段を用いて、指定した所有者AIDと指定したすべての会員AIDを連結する。

【0264】4. 仮AIDと同様に、任意の手段で仮PATを生成する(ステップS4414)。

【0265】5. 生成したAIDリストを生成した仮PATの定められた範囲に複写する(ステップS4415)。

【0266】6. AIDリストを複写した仮PATに、所有者インデックスの値を書き込む(ステップS4416)。

【0267】7. 所有者インデックスの値を書き込んだ仮PATに、移転制御フラグの値を書き込む(ステップS4417)。

【0268】8. 移転制御フラグの値を書き込んだ仮PATに、有効期限の値を書き込む(ステップS4418)。

【0269】9. 有効期限の値を書き込んだ仮PATに、PAT演算装置の識別子を書き込む(ステップS4419)。

【0270】10. PAT演算装置の識別子を書き込んだ仮PATに、PAT演算装置の秘密鍵で署名する(ステップS4420)。

【0271】次に、図22のフローチャートを参照し

て、SplitPATの手順について説明する。

【0272】1. 所有者AIDを指定する(ステップS4511)。

【0273】2. 分割後のPATの会員AIDとするAIDをすべて指定する(ステップS4512)。

【0274】3. 指定した所有者AIDと指定したすべての会員AIDからAIDリストを生成する(ステップS4513)。具体的には、任意の手段を用いて、指定した所有者AIDと指定したすべての会員AIDを連結する。

【0275】4. 仮AIDと同様に、任意の手段で仮PATを生成する(ステップS4514)。

【0276】5. 生成したAIDリストを生成した仮PATの定められた範囲に複写する(ステップS4515)。

【0277】6. AIDリストを複写した仮PATに、所有者インデックスの値を書き込む(ステップS4516)。

【0278】7. 所有者インデックスの値を書き込んだ仮PATに、移転制御フラグの値を書き込む(ステップS4517)。

【0279】8. 移転制御フラグの値を書き込んだ仮PATに、有効期限の値を書き込む(ステップS4518)。

【0280】9. 有効期限の値を書き込んだ仮PATに、PAT演算装置の識別子を書き込む(ステップS4519)。

【0281】10. PAT演算装置の識別子を書き込んだ仮PATに、PAT演算装置の秘密鍵で署名する(ステップS4520)。

【0282】11. 分割を継続する場合には(ステップS4521YES)、2. に戻り、10. までは順番に実行する。

【0283】なお、図21、図22の手順において、AIDリストの生成は、図23のフローチャートにより次のように行う。すなわち、まずバッファ長を決定し(ステップS4611)、バッファを生成する(ステップS4612)。次いで、所有者AIDを生成したバッファの空き領域にコピーする(ステップS4613)。次いで、会員AIDをバッファの空き領域にコピーし(ステップS4614)、次の会員AIDが存在すれば(ステップS4615YES)ステップS4614を繰り返す。

【0284】次に、所有者AIDの決定について説明す

る。MakePAT, MergePAT, SplitPAT, TransPAT各命令は、2個以上の引数を持ち、引数として、役割識別子AID、個別化アクセスチケットPAT、または、Enableを指定できると定義する。この時、PAT演算装置は、各命令実行後に出力されるPATの所有者AIDをそれぞれ下記の規則に従い指定する。

【0285】・MakePATの場合

MakePAT命令に対して、第1引数から第N引数(N=2, 3, ...)までAIDを、第N+1引数以降ではEnablerを指定すると定義する。例えば、

MakePAT AID₁ AID₂ ... AID_N Enabler of AID₁

Enabler of AID₂ ... Enabler of AID_N

—PAT演算装置は、MakePAT命令の第1引数のAIDを所有者AIDであると解釈する。

【0286】—第N+1引数以降のEnablerのいずれかが第1引数のAIDに対応している場合に限り、PAT演算装置はこのAID(すなわち、第1引数のAID)をMakePAT命令実行後に出力されるPATの所有者AIDに指定する。

【0287】・MergePATの場合

SplitPAT PAT₁ (AID₁₁) (AID₂₁ AID₂₂) ...
(AID_{N1} AID_{N2} ... AID_{NN}) Enabler of AID

—PAT演算装置は、SplitPAT命令の第1引数のPATの所有者AIDを、SplitPAT命令実行後に出力されるPATの所有者AIDであると解釈する。

【0290】—第N+1引数のEnablerが第1引数のPATの所有者AIDに対応している場合に限り、PAT演算装置はこのAID(すなわち、第1引数のPATの

TransPAT PAT₁ PAT₂ AID

Enabler of AID₁ Enabler of AID₂

—PAT演算装置は、TransPAT命令の第3引数のAIDが第2引数のPATに含まれている場合に限り、第3引数のAIDを、TransPAT命令実行後に出力されるPATの所有者AIDであると解釈する。

【0292】—第4引数のEnablerが第1引数のPAT及び第2引数のPATの両者に対応しており、かつ、第5引数のEnablerが第3引数のAIDに対応している場合に限り、PAT演算装置は第3引数のAIDをTransPAT命令実行後に出力されるPATの所有者AIDに指定する。

【0293】次に、会員AIDの決定について説明する。MakePAT, MergePAT, SplitPAT, TransPAT各命令の定義は上に従う。PAT演算装置は、各命令実行後に出力されるPATの会員AIDをそれぞれ下記の規則に従い指定する。

【0294】・MakePATの場合

MakePAT命令実行後に出力されるPATの所有者AIDが正式に決定された場合に限り、

—PAT演算装置は、MakePAT命令の第2引数以降の

MergePAT命令に対して、第1引数から第N引数(N=2, 3, ...)までPATを、第N+1引数ではEnablerを指定すると定義する。すなわち、

MergePAT PAT₁ PAT₂ ... PAT_N Enabler of AID

—PAT演算装置は、MergePAT命令の第1引数のPATの所有者AIDを、MergePAT命令実行後に出力されるPATの所有者AIDであると解釈する。

【0288】—第N+1引数のEnablerが第1引数のPATの所有者AIDに対応している場合に限り、PAT演算装置はこのAID(すなわち、第1引数のPATの所有者AID)をMergePAT命令実行後に出力されるPATの所有者AIDに指定する。

【0289】・SplitPATの場合

SplitPAT命令に対して、第1引数でPATを、第2引数から第N引数(N=3, 4, ...)まではあらかじめ定められた何らかの記号(この例ではカッコ())とする)でまとめられた1個以上のAIDのまとまりを、第N+1引数ではEnablerを指定すると定義する。すなわち、

所有者AID)をSplitPAT命令実行後に出力されるPATの所有者AIDに指定する。

【0291】・TransPATの場合

TransPAT命令に対して、第1引数及び第2引数でPATを、第3引数でAIDを、第4引数及び第5引数ではEnablerを指定すると定義する。すなわち、

すべてのAIDをMakePAT命令実行後に出力されるPATの会員AIDであると解釈する。

【0295】—第2引数以降のすべてのAIDのうち、第N+1引数以降で指定されたEnablerと対応しているAIDのみ、PAT演算装置はMakePAT命令実行後に出力されるPATの会員AIDに指定する。

【0296】・MergePATの場合

PAT演算装置は、MergePAT命令実行後に出力されるPATの所有者AIDが正式に決定された場合に限り、MergePAT命令の第1引数から第N引数で指定されたすべてのPATの会員AIDを、MergePAT命令実行後に出力されるPATの会員AIDに指定する。

【0297】・SplitPATの場合

PAT演算装置は、SplitPAT命令実行後に出力されるPATの所有者AIDが正式に決定された場合に限り、SplitPAT命令の第1引数で指定されたPATの会員AIDを、SplitPAT命令実行後に出力されるPATの会員AIDに指定する。このとき、会員AIDはカッコ()単位で別々のPATに振り分けられる。例え

ば、

$$\text{SplitPAT } \text{PAT}(\text{AID}_{11}) (\text{AID}_{21} \text{ AID}_{22}) \dots$$

$$(\text{AID}_{N1} \text{ AID}_{N2} \dots \text{AID}_{NM}) \text{ Enabler of AID}$$

の場合、 (AID_{11}) と $(\text{AID}_{21} \text{ AID}_{22})$ と $(\text{AID}_{N1} \text{ AID}_{N2} \dots \text{AID}_{NM})$ は所有者AIDが共通な別のPATの会員AIDになる。

【0298】・TransPATの場合

PAT演算装置は、TransPAT命令実行後に出力されるPATの所有者AIDが正式に決定された場合に限る、TransPAT命令の第1引数で指定されたPATのすべての会員AID及び第2引数で指定されたPATの会員AIDのうち新所有者AIDとなる予定の会員AIDを除いた残りのすべての会員AIDを、TransPAT命令実行後に出力されるPATの会員AIDに指定する。

【0299】次に、Enablerの正当性の検証について説明する。このEnablerの正当性の検証は、MakePAT、MergePAT、SplitPAT、TransPATで共通であり、図24に示すように行われる。

【0300】1. AIDとEnablerを入力する(ステップS5511)。

【0301】2. この入力されたAIDとEnablerをそれぞれ認証局CAの公開鍵で検証する(ステップS5512)。少なくとも一方が改竄されている場合には(ステップS5513YES)、処理を終了する。

【0302】3. Enablerであることを証明する文字列を入力する(ステップS5514)。

【0303】4. ステップS5511のEnablerの先頭フィールドとステップS5514の文字列を比較する(ステップS5515)。一致しない場合には(ステップS5516NO)、処理を終了する。

【0304】5. 一致する場合には(ステップS5516YES)、ステップS5511のAIDとEnabler中のAIDを比較する(ステップS5517)。

【0305】6. 比較結果を出力する(ステップS5519)。

【0306】次に、図25～図28を参照して、本発明の第3の実施形態について説明する。

【0307】上述した実施形態における個別化アクセスチケット(PAT)の新規生成(MakePAT)および所

有者変更(TransPAT)では、会員AIDとEnabler of 会員AIDを個別化アクセスチケットの所有者に渡すことが必要であるが、これを所有者に渡すと、その所有者が別の所有者の主催するグループ通信に対して、取得した会員AIDで参加することが可能になる。すなわち、会員AIDを用いた成りすましが可能になるという問題がある。また、その所有者が取得した会員AIDおよびEnabler of 会員AIDを不特定多数が閲覧可能なメディアに掲載すれば、誰でもその会員AIDにアクセス可能になるため、会員AIDのユーザへの嫌がらせが発生する恐れがあるとともに、また第三者による会員AIDを用いた成りすましも可能になるという問題がある。

【0308】そこで、本実施形態では、Enabler of 会員AIDを所有者に渡さなくても、MakePATおよびTransPATを可能にする。

【0309】このために、本実施形態では、Null-AID(AID_{Null})および該Null-AIDのEnabler(Enabler of Null-AIDまたはEnabler of AID_{Null})を使用して、個別化アクセスチケット(PAT)の新規生成および既存の個別化アクセスチケット(PAT)の内容変更を行うものである。ここで、Null-AIDを含む演算は、以下のすべての規則に従う：

(a) 上述した実施形態における新規生成(MakePAT)、マージ(MergePAT)、分割(SplitPAT)、変更(TransPAT)からなる演算規則、(b) Null-AIDにのみ適用可能な規則として、i. Null-AIDは、すべてのユーザに既知であり、ii. Enabler of Null-AIDは、すべてのユーザに既知である。

【0310】ここで、上述した実施形態で定義した演算規則について説明する。

【0311】(1) 複数AIDからPATを作る(MakePAT)：

【数8】

$$\begin{aligned} & \text{AID}_{\text{holder}} + \text{AID}_{\text{member1}} + \text{AID}_{\text{member2}} + \dots + \text{AID}_{\text{memberN}} \\ & + \text{Enabler of AID}_{\text{member1}} + \text{Enabler of AID}_{\text{member2}} + \dots \\ & + \text{Enabler of AID}_{\text{memberN}} + \text{Enabler of AID}_{\text{holder}} \\ \rightarrow & \text{PAT} < \text{AID}_{\text{holder}} | \text{AID}_{\text{member1}}, \text{AID}_{\text{member2}}, \dots, \\ & \text{AID}_{\text{memberN}} > \end{aligned}$$

【数9】

(2) 同一所有者の複数PATをマージする(MergePAT)：

$$\begin{aligned} & \text{PAT} < \text{AID}_{\text{holder}} | \text{AID}_{\text{membera1}}, \text{AID}_{\text{membera2}}, \dots, \\ & \text{AID}_{\text{memberaM}} > \\ & + \text{PAT} < \text{AID}_{\text{holder}} | \text{AID}_{\text{memberb1}}, \text{AID}_{\text{memberb2}}, \dots, \end{aligned}$$

AID_{memberbN}>
 + Enabler of AID_{holder}
 → PAT<AID_{holder} | AID_{membera1}, AID_{membera2}, ...,
 AID_{memberaM}, AID_{memberb1}, AID_{memberb2}, ...,
 AID_{memberbN}>

(3) PATを同一所有者の複数PATに分割する (SplitPAT) : 【数10】

PAT<AID_{holder} | AID_{membera1}, AID_{membera2}, ...,
 AID_{memberaM}, AID_{memberb1}, AID_{memberb2}, ...,
 AID_{memberbN}>
 + Enabler of AID_{holder}
 → PAT<AID_{holder} | AID_{membera1}, AID_{membera2}, ...,
 AID_{memberaM}>
 + PAT<AID_{holder} | AID_{memberb1}, AID_{memberb2}, ...,
 AID_{memberbN}>

(4) PATの所有者AIDを変更する (TransPAT) : 【数11】

PAT<AID_{holder} | AID_{membera1}, AID_{membera2}, ...,
 AID_{memberaM}> + PAT<AID_{holder} | AID_{newholder}>
 + Enabler of AID_{holder} + Enabler of AID_{newholder}
 → PAT<AID_{newholder} | AID_{membera1}, AID_{membera2}, ...,
 AID_{memberaM}>

Null-AIDを含むPATへの有効期限の値及び移転制御フラグの値の指定方法は、上述した第2の実施形態における有効期限の値及び移転制御フラグの値の指定方法に従う。

【0312】次に、Null-AIDに関する演算例について説明する。

AID_{Null} + AID_A + Enabler of AID_A + Enabler of AID_{Null}
 → PAT<AID_{Null} | AID_A>

(2) PAT<AID_{Null} | AID_A>とPAT<AID_{Null} | AID_B>とからPAT<AID_{Null} | AID_A, AID_B>を作る場合:

(a) Null-AIDの規則(b)i. および(b)ii.より、

PAT<AID_{Null} | AID_A> + PAT<AID_{Null} | AID_B>
 + Enabler of AID_{Null}
 → PAT<AID_{Null} | AID_A, AID_B>

(3) PAT<AID_{Null} | AID_A>とPAT<AID_{Null} | AID_B>と Enabler of AID_A とからPAT<AID_A | AID_B>を作る場合:

(a) Null-AIDの規則(b)i. および(b)ii.より、

PAT<AID_{Null} | AID_A> + PAT<AID_{Null} | AID_B>
 + Enabler of AID_{Null} + Enabler of AID_A
 → PAT<AID_A | AID_B>

Null-AIDのデータ構造は、図25に示すように、Null-AIDであることを一意に表す文字列 (例えば、この文字列は認証局CAで定義される) および該文字列に対して認証局CAの署名を施したもので構成される。

【0317】また、Enabler of Null-AIDのデ

【0313】(1) AID_A と Enabler of AID_A とからPAT<AID_{Null} | AID_A>を作る場合:

(a) Null-AIDの規則(b)i. および(b)ii.より、AID_{Null}と Enabler of AID_{Null}は既知である。

【0314】(b) MakePATにより

【数12】

AID_{Null}と Enabler of AID_{Null}は既知である。

【0315】(b) MergePATにより

【数13】

AID_{Null}と Enabler of AID_{Null}は既知である。

【0316】(b) TransPATにより

【数14】

ータ構造は、図26に示すように、Enabler であることを一意に表す文字列 (例えば、この文字列は認証局CAで定義される)、Null-AIDの実体、および前記 Enabler であることを表す文字列と前記Null-AIDの実体を連結した文字列に対して認証局CAの署名を施したもので構成される。

【0318】なお、Null-AIDおよび Enabler of Null-AIDは、セキュアなPAT演算装置およびセキュアなPAT認証局で保持される。

【0319】次に、本実施形態の第1の応用例について図27を参照して説明する。図27においては、以下の動作を行う。

【0320】(1) ユーザB (PAT会員) は、ユーザBの端末と接続されたセキュアなPAT演算装置で前記Null-AIDに関する演算例(1)を実行してPAT<AID_{Null} | AID_B>を生成し、任意の手段でユーザA (PAT所有者) に渡す。

【0321】(2) PAT<AID_{Null} | AID_B>を受信したユーザAは、ユーザAの端末に接続されたセキュアなPAT演算装置で

(a) Null-AIDに関する演算例(1)を実行してPAT<AID_{Null} | AID_A>を作る。

【0322】(b) Null-AIDに関する演算例(3)を実行してPAT<AID_A | AID_B>を作る。

【0323】(3) ユーザAは、生成したPAT<AID_A | AID_B>を任意の手段でユーザBに渡す。

【0324】なお、有効期限の決定方法は前述した方法と共通のため省略する。また、Null-AIDに関する演算の処理は前述した方法と共通のため省略する。

【0325】PAT<AID_{Null} | AID_A, AID_B>をユーザBに渡す場合には、上述した動作(2)において、前記Null-AIDに関する演算例(2)を実行する。

【0326】次に、本実施形態の第2の応用例について図28を参照して説明する。図28においては、以下の動作を行う。

【0327】(1) ユーザB (PAT会員) は、ユーザBの端末と接続されたセキュアなPAT演算装置でNull-AIDに関する演算例(1)を実行してPAT<AID_{Null} | AID_B>を作り、任意の公開情報とともにアノニマス・ディレクトリ・サービスADSに登録する。

【0328】(2) ユーザA (PAT所有者) は、ユーザAの端末に接続されたセキュアなPAT演算装置でNull-AIDに関する演算例(1)を実行してPAT<AID_{Null} | AID_A>を作り、任意の検索条件とともにアノニマス・ディレクトリ・サービスADSに提示する。

【0329】(3) ユーザBの個人情報がユーザAの提示した検索条件を満足した場合、アノニマス・ディレクトリ・サービスADSに接続されたセキュアなPAT演算装置は

(a) Null-AIDに関する演算例(2)を実行してPAT<AID_{Null} | AID_A, AID_B>を作る。

【0330】(b) PAT<AID_{Null} | AID_A, AID_B>をアノニマス・ディレクトリ・サービスADSに渡す。

【0331】(4) アノニマス・ディレクトリ・サービスADSは、PAT演算装置で作られたPAT<AID_{Null} | AID_A, AID_B>をユーザAに渡す。

【0332】(5) PAT<AID_{Null} | AID_A, AID_B>を受け取ったユーザAは、ユーザAの端末に接続されたセキュアなPAT演算装置で下記のTransPAT演算を実行して、PAT<AID_A | AID_B>を作る。

【0333】

【数15】
PAT<AID_{Null} | AID_A>
+ PAT<AID_{Null} | AID_A, AID_B>
+ Enabler of AID_{Null} + Enabler of AID_A
→ PAT<AID_A | AID_B>

尚、有効期限の決定方法は前述した方法と共通のため省略する。また、Null-AIDに関する演算の処理は前述した方法と共通のため省略する。

【0334】PAT<AID_A | AID_B>をアノニマス・ディレクトリ・サービスADSに接続されたセキュアなPAT演算装置で生成する場合には、そのPAT演算装置に Enabler of AID_A を渡す。そして、上述した動作(3)において、Null-AIDに関する演算例(3)を実行する。

【0335】PAT<AID_B | AID_A>をアノニマス・ディレクトリ・サービスADSに接続されたセキュアなPAT演算装置で生成して、ユーザBに渡す場合には、そのPAT演算装置に Enabler of AID_B を渡す。そして、上述した動作(3)において、Null-AIDに関する演算例(3)と同様の演算を実行する。

【0336】次に、本発明の第4の実施形態について図29～図31を参照して説明する。グループ通信においては参加者を固定したい状況はしばしば発生するが、上述した実施形態では個別化アクセスチケット (PAT) を変更不可にする機能を持たないため、参加者を固定することができない。すなわち、上述した実施形態では、参加者を固定するか否かは、個別化アクセスチケットの所有者の判断に一任されている。

【0337】そこで、本実施形態では、個別化アクセスチケットに読取専用属性を設定している。

【0338】このため、本実施形態では、God-AID (AID_{God}) を用いて、個別化アクセスチケット (PAT) に読取専用属性を設定している。ここで、God-AIDに関する演算は、以下のすべての規則に従う：

(a) God-AIDは、すべてのユーザに既知であり、
(b) God-AIDに関する演算は、以下のいずれかのみ許可される：

【数16】

i. AID_{holder} が AID_{Null} でも AID_{God} でもない場合:
 $PAT < AID_{holder} | AID_{member1}, AID_{member2}, \dots, AID_{memberN} >$

+ Enabler of AID_{holder}
 $\rightarrow PAT < AID_{God} | AID_{holder}, AID_{member1}, AID_{member2}, \dots, AID_{memberN} >$

ii. AID_{holder} が AID_{Null} の場合:

$PAT < AID_{Null} | AID_{member1}, AID_{member2}, \dots, AID_{memberN} >$
 + Enabler of AID_{Null}
 $\rightarrow PAT < AID_{God} | AID_{member1}, AID_{member2}, \dots, AID_{memberN} >$

God-AID のデータ構造は、図 29 に示すように、God-AID であることを一意に表す文字列 (例えば、この文字列は認証局 CA で定義される) および該文字列に対して認証局 CA の署名を施したものから構成される。God-AID は、上述したセキュアな PAT 演算装置およびセキュアな PAT 認証局で保持されている。

【0339】Null-AID を含む PAT の処理は、図 21-図 24 に従う。所有者 AID が Null-AID でも God-AID でもない場合には、AID リストに God-AID を付加し、所有者インデックスの値を God-AID 付加後の AID リストにおける God-AID の位置と等しくなるように指定する。所有者 AID が Null-AID の場合には、AID リストから N

$PAT < AID_{Null} | AID_A > + PAT < AID_{Null} | AID_B >$
 + Enabler of AID_{Null}
 $\rightarrow PAT < AID_{Null} | AID_A, AID_B >$

(2) God-AID に関する演算規則 (a) より、 AID_{God} は既知である。

(3) God-AID に関する演算規則 (b) ii. より

【数 18】

$PAT < AID_{Null} | AID_A, AID_B >$
 + Enabler of AID_{Null}
 $\rightarrow PAT < AID_{God} | AID_A, AID_B >$

上記演算は、第三者の計算機 (サーチエンジンなど) に接続されたセキュアな PAT 演算装置 (図 31) またはセキュアな PAT 認証局でも実行される。

【0343】次に、図 32 を参照して、本発明の第 5 の実施形態について説明する。

【0344】上述した第 3 の実施形態で説明したように Null-AID を追加すると、以下に説明するように、個別化アクセスチケット (PAT) の所有者 (所有者 AID のユーザ) が会員 (会員 AID のユーザ) へのアクセス権を第三者に譲渡できるようになるという問題がある。しかも、会員に無断で譲渡可能である。

$AID_A + AID_{Null} + \text{Enabler of } AID_{Null} + \text{Enabler of } AID_A$
 $\rightarrow PAT < AID_A | AID_{Null} >$

(b) A は、TransPAT により、 $PAT < AID_{Null} |$

$AID_{Null} >$ を削除し、次に God-AID を付加し、最後に所有者インデックスの値を God-AID 付加後の AID リストにおける God-AID の位置と等しくなるように指定する。

【0340】次に、本実施形態の応用例について図 30 を参照して説明する。

【0341】 $PAT < AID_{Null} | AID_A >$ と $PAT < AID_{Null} | AID_B >$ とから $PAT < AID_{God} | AID_A, AID_B >$ を作る場合、PAT 所有者 (図 30 におけるユーザ A) の端末に接続されたセキュアな PAT 演算装置において、以下の演算を実行する。

【0342】(1) 上述した MergePAT により

【数 17】

【0345】1. $PAT < AID_A | AID_B >$ の所有者 A が (会員は B)

・ $PAT < AID_A | AID_B >$
 ・ AID_A
 ・ Enabler of AID_A

を用いて、 $PAT < AID_{Null} | AID_B >$ を作る。ここで、A は、 $PAT < AID_A | AID_B >$ に加えて

・ AID_A
 ・ Enabler of AID_A
 ・ AID_{Null}
 ・ Enabler of AID_{Null}

をすべて知っているとする。

【0346】(a) A は、MakePAT により、 $PAT < AID_A | AID_{Null} >$ を作る。

【0347】

【数 19】

$AID_B >$ を作る。

【0348】

PAT<AID_A | AID_B>+PAT<AID_A | AID_{Null}>
 + Enabler of AID_A + Enabler of AID_{Null}
 →PAT<AID_{Null} | AID_B>

上記1. (b) の後、AがPAT<AID_{Null} | AID_B>を第三者Cに渡すと次の2. が可能となる。

【0349】2. Cは、PAT<AID_{Null} | AID_B>を用いて、PAT<AID_C | AID_B>を作る。ここで、Cは、PAT<AID_{Null} | AID_B>に加えて
 ・ AID_C
 ・ Enabler of AID_C

AID_{Null}+AID_C + Enabler of AID_C + Enabler of AID_{Null}
 → PAT<AID_{Null} | AID_C>

(b) Cは、TransPATにより、PAT<AID_C | AID_B>を作る。

PAT<AID_{Null} | AID_B>+PAT<AID_{Null} | AID_C>
 + Enabler of AID_{Null}+ Enabler of AID_C
 → PAT<AID_C | AID_B>

上記2 (b) の結果、CはPAT<AID_C | AID_B>を得るので、Bへのアクセスが可能になる。

【0353】そこで、本実施形態では、PAT<AID_{holder} | AID_{member}>の所有者がAID_{member}のEnablerを知らない場合には、このPATからPAT<AID_{Null} | AID_{member}>を作ることができないようにする。

【0354】上述した第3の実施形態では、PATの所有者がAID_{member}のEnabler なしでPAT<AID_{Null} | AID_{member}>を作るためには、PAT<AID_{holder} | AID_{Null}>を作ることが必要になる。

【0355】そこで、本実施形態では、上述した第3の実施形態で説明したNull-AIDに対して、以下の規則を追加する。

【0356】Null-AIDはPATの所有者AIDとしてのみ使用できる（会員AIDとしては使用できない）。

【0357】・PAT<AID_{Null} | AID_{member1}, AID_{member2}, ..., AID_{memberN}>は許可する。

【0358】・PAT<AID_{holder} | AID_{Null}, AID_{member1}, AID_{member2}, ..., AID_{memberN}>は許可しない。

【0359】上述した実施形態におけるセキュアなPAT演算装置とセキュアなPAT認証局にそれぞれNull-AIDが会員AIDに含まれているか否かをチェックする機能を追加する。この会員AIDのチェック処理機能について図32に示すフローチャートを参照して説明する。

【0360】1. Null-AIDとPATを入力する（ステップS6911）。

【0361】2. ステップS6911で入力したPATから、会員AIDをすべて取り出す（ステップS691

【数20】

・ AID_{Null}
 ・ Enabler of AID_{Null}
 をすべて知っているとする。

【0350】(a) Cは、MakePATにより、PAT<AID_{Null} | AID_C>を作る。

【0351】

【数21】

【0352】

【数22】

3)。

【0362】3. この取り出したすべての会員AIDについて、それぞれ、ステップS6911で入力したNull-AIDと比較する（ステップS6915）。

【0363】・すべての会員AIDがNull-AIDと完全に一致しない場合（ステップS6917NO、S6919NO）、MergePAT、SplitPAT、またはTransPAT処理に移る（図21または図22）（ステップS6921）。

【0364】・会員AIDが1つでもNull-AIDと完全に一致する場合（ステップS6917YES）、処理を終了する。

【0365】次に、図33～図39を参照して、本発明の第6の実施形態について説明する。この第6の実施形態は、上述した第1の実施形態において図2に示した役割識別子AIDに対して図34 (b) のようにリンク情報を追加するとともに、図2に示した1対1個別化アクセスチケットPATに含まれていた役割識別子AIDの実体の代わりに前記役割識別子AIDのリンク情報を図34 (c) に示すように設定し、該リンク情報で役割識別子AIDを一意に特定するように構成した点が異なるものである。

【0366】なお、このようにリンク情報を追加された役割識別子AIDをリンク情報付き役割識別子AIDと称し、AIDのリンク情報を有する1対1個別化アクセスチケットPATをリンク指定型1対1個別化アクセスチケットPATと称することにする。また、リンク情報は、役割識別子AIDを一意に特定可能な情報であり、一般に識別子と呼ばれる種類のデータで、例えば認証局CAによって役割識別子AIDに対して一意に付与されるシリアル番号である。

【0367】まず、図33を参照して、本発明の第6の

実施形態の全体構成図について説明する。図33において、1は認証局CAであり、個人識別子OIDの認証権限と役割識別子AIDの発行権限を有し、ユーザに対して役割識別子を割り当てる機能を有する。3はユーザであり、5はセキュア・コミュニケーション・サービスSCSであり、ユーザ3間の電子メールを転送し、必要に応じて着信拒否および個人識別子の同一性を判定し、取り出す。7はアノニマス・ディレクトリ・サービスADSであり、役割識別子AID、移転制御フラグの値、有効期限の値、および、公開情報を管理するデータベースである。すなわち、アノニマス・ディレクトリ・サービスADS7は、検索者の役割識別子AIDと検索条件を満足する登録者の役割識別子AIDから個別化アクセスチケットPATを生成し、検索者に発行する機能を有する。

【0368】ユーザの要求に基づいて個人識別子から役割識別子AIDを生成し、そのユーザに割り当てるまでの一連の処理はリンク情報が付加されることを除いて第1の実施形態と基本的に同じであるが、具体的に図34を参照して説明する。

【0369】図34は、個人識別子OID(Official Identification)とリンク情報付き役割識別子AIDとリンク指定型1対1個別化アクセスチケットPATの例を示している。個人識別子OIDは、図34(a)に示すように、認証局CA1がユーザを一意に識別可能な規則に従う任意の文字列と公開鍵から構成される情報に対し、認証局CA1が署名したものである。また、リンク情報付き役割識別子AIDは、図34(b)に示すように、個人識別子OIDの断片とその位置情報、冗長な文字列、SCSを動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列(ホスト名、実ドメイン等)、およびリンク情報から構成される情報に対し、認証局CA1が署名したものである。

【0370】また、リンク指定型1対1個別化アクセスチケットPATは、図34(c)に示すように、移転制御フラグ、役割識別子AID₀のリンク情報、役割識別子AID₁のリンク情報、有効期限から構成される情報に対してアノニマス・ディレクトリ・サービスADSが署名したものである。

【0371】ユーザ3がリンク情報付き役割識別子AIDを認証局CA1に対して要求する処理は、第1の実施形態において前述したものと同一である。

【0372】次に、上述した役割識別子AIDの要求に対する認証局CA1が役割識別子AIDをユーザ3に対して交付する処理も第1の実施形態において前述したものと同一である。

【0373】次に、認証局CAにおけるリンク情報付き役割識別子AIDの生成処理について図35を参照して説明する。図35において、認証局CAは個人識別子OIDの全長Lと等しい長さの情報を生成する。この情報

を仮の役割識別子AIDとする(ステップS7211)。次に、個人識別子OIDの部分複写を行うために、個人識別子OIDの複写範囲を指定するパラメータ p_i と l_i の値をそれぞれ乱数発生等の任意の手段を用いて決定する(ステップS7213)。ここで、Lは個人識別子OIDの全長と等しく、 l_i は $0 \leq l_i \leq L$ の関係が成立する範囲で任意に定めた値とする。次に、個人識別子OIDの先頭から位置 p_i から位置 $p_i + l_i$ の範囲の情報を、仮AIDの同じ位置に複写する(ステップS7215)。つまり、このOID断片は仮AIDの先頭から位置 p_i と位置 $p_i + l_i$ の範囲に複写される。次に、OIDを部分複写した仮AIDの定められた範囲に、 p_i と l_i の値を任意の手段で暗号化して書き込む(ステップS7217)。次に、これらの値を書き込んだ仮AIDの定められた範囲にセキュア・コミュニケーション・サービスSCS5を動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列(ホスト名、実ドメイン名等)を書き込む(ステップS7219)。次に、リンク情報を付加する(ステップS7220)。そして、このように文字列およびリンク情報を書き込んだ仮AIDに認証局CA1の秘密鍵で署名する(ステップS7221)。

【0374】次に、ユーザB3の役割識別子AID及び公開情報をアノニマス・ディレクトリ・サービスADS7に登録する手続きについて説明する。登録者であるユーザB3とアノニマス・ディレクトリ・サービスADS7との間で、ユーザB3の役割識別子AIDとADS7の証明書を用いて、任意の手段で双方向認証を行う。次に、ユーザB3は、移転制御フラグの値、有効期限の値、及び、趣味などの公開情報をADS7に送信する。次に、ADS7はユーザB3から受信した移転制御フラグの値、有効期限の値、すべての公開情報を、すべてユーザB3のAIDと関連付けて記憶装置に記録する。

【0375】なお、上記手続きにおいて、登録者であるユーザB3とADS7間の通信を暗号化する場合もある。

【0376】次に、ユーザA3がアノニマス・ディレクトリ・サービスADS7に登録された公開情報を検索する手続きについて説明する。検索者であるユーザA3とアノニマス・ディレクトリ・サービスADS7との間で、ユーザA3のAIDとADS7の証明書を用いて、任意の手段で双方向認証を行う。次に、ユーザA3は、任意の検索条件をアノニマス・ディレクトリ・サービスADS7に送信する。次に、アノニマス・ディレクトリ・サービスADS7は、受信したすべての検索条件を記憶装置に提示し、これらの検索条件を満足する登録者の役割識別子AIDを抽出する。次に、アノニマス・ディレクトリ・サービスADS7はユーザA3の役割識別子AIDのリンク情報と検索条件を満足した登録者の役割識別子AIDのリンク情報と移転制御フラグの値と有効

期限の値からリンク指定型1対1個別化アクセスチケットPATを生成する。次に、ADS7は、生成したPATをユーザA3に送信する。

【0377】なお、上記手続きにおいて、検索者であるユーザA3とADS7間の通信を暗号化する場合もある。

【0378】リンク指定型1対1個別化アクセスチケットは、アノニマス・ディレクトリ・サービスADS7の検索結果として生成する。

【0379】次に、図36のフローチャートを参照して、ADSにおけるリンク指定型1対1個別化アクセスチケットPATの生成処理について説明する。まず、ある定められた長さの情報を生成する。これを仮の個別化アクセスチケット（仮PAT）とする（ステップS7510）。次に、検索者であるユーザA3の役割識別子AIDのリンク情報と登録者であるユーザB3の役割識別子AIDのリンク情報を仮PATの定められた範囲に複写する（ステップS7516）。次に、移転制御フラグの値と有効期限の値をそれぞれ、AIDのリンク情報を複写した仮PATの定められた範囲に書き込む（ステップS7517）。次に、これらの値を書き込んだ仮PATにADSの秘密鍵で署名する（ステップS7519）。

【0380】次に、リンク指定型1対1個別化アクセスチケットPATによる移転制御について説明する。移転制御とは、PATを譲渡されたあるいは盗聴した第三者（本来はアクセス権を有していないユーザ）から、正当なアクセス権を持つユーザへのアクセスを制限する機能である。

【0381】アノニマス・ディレクトリ・サービスADS7及び登録者AIDのユーザB3は、個別化アクセスチケットPATの移転制御フラグにある値を設定することにより、アクセス権を有していない第三者からのユーザB3への接続を禁止することができる。

【0382】移転制御フラグの値を1に設定した場合には、セキュア・コミュニケーション・サービスSCS5と発信者との間で任意のチャレンジ/レスポンス方式に従い発信者役割識別子AIDを認証するため、発信者が発信者AIDとPATの両者を発信者以外のいかなるユーザに渡しても、そのユーザは登録者にSCS5を介して接続できない。

【0383】一方、移転制御フラグの値を0に設定した場合には、SCS5と発信者との間でいかなるチャレンジ/レスポンスも行わないため、発信者が発信者AIDとPATの両者を発信者以外のユーザに渡したら、それらのユーザもアノニマス・ディレクトリ・サービスの登録者とSCS5を介して接続できるようになる。

【0384】次に、図37を参照してSCSにおけるメールアクセス制御方法について説明する。

【0385】発信者はFrom:行に” 発信者AID@ 発信者のSCSの実ドメイン”、To:行に” PAT@

発信者のSCSの実ドメイン”の形式で指定する。

【0386】SCSはSMTP(Simple Mail Transfer Protocol)等のMTA(Message Transfer Agent)の受信したメールを取得し、図37に示す処理を実行する。

【0387】1. PATの署名をADSの公開鍵を用いて検証する(ステップS7713)。

【0388】・PATの署名に改竄が認められる場合(ステップS7715YES)、メールを破棄して終了する(ステップS7716)。

【0389】・PATの署名に改竄が認められない場合(ステップS7715NO)、下記処理2.を実行する。

【0390】2. 発信者AIDのリンク情報をPATに提示して検索する(ステップS7717、S7720、S7722)。

【0391】・発信者AIDのリンク情報と完全一致するリンク情報がPATに含まれていない場合には(ステップS7723NO)、メールを破棄して終了する(ステップS7716)。

【0392】・発信者AIDのリンク情報と完全一致するリンク情報がPATに含まれている場合には(ステップS7723YES)、下記処理3.を実行する。

【0393】3. PATの有効期限の値を評価する(ステップS7725、S7727)。

【0394】・PATが有効期間外の場合には(ステップS7727NO)、メールを破棄して終了する(ステップS7716)。

【0395】・PATが有効期限内の場合には(ステップS7727YES)、下記処理4.を実行する。

【0396】4. PATの移転制御フラグの値を参照して、発信者を認証するか否かを決定する(ステップS7731、S7733)。

【0397】・値が1の場合には(ステップS7733YES)、SCSはリンク情報を認証局CAに提示して発信者AIDの実体及び発信者AIDの公開鍵を取得し、SCSと発信者との間でチャレンジ/レスポンス認証を実行して、発信者の署名を確認する(ステップS7735)。署名が正しい場合には、着信者を指定し、PATを添付する(ステップS7737)。署名が正しくない場合には、メールを廃棄して終了する(ステップS7716)。

【0398】・値が0の場合には(ステップS7733NO)、チャレンジ/レスポンス認証を実行せずに着信者を指定し、PATを添付する(ステップS7737)。

【0399】SCSと発信者との間のチャレンジ/レスポンス方法は1対1個別化アクセスチケットに対するチャレンジ/レスポンス方法と同様である。

【0400】次に、SCSにおける着信者の指定方法について説明する。

【0401】SCSは、まず、発信者AIDのリンク情報をPATに提示して検索し、発信者AIDのリンク情報と完全一致しないすべてのリンク情報を取得する。次に、取得したすべてのリンク情報を認証局CAに提示して検索し、AIDを取得する。取得したすべてのAIDを以後、着信者AIDと定義する。次に、取得したすべてのAIDについて、それぞれ、着信者AIDから着信者のSCSの実ドメインを取り出す。次に、着信者を“着信者AID@着信者のSCSの実ドメイン”の形式で指定する。最後に、SCSは発信者を“発信者AID@発信者のSCSの実ドメイン”の形式から“発信者AID”の形式に変更する。

【0402】SCSにおけるPATの添付方法は、1対1個別化アクセスチケットに対する添付方法と同様である。

【0403】次に、SCSにおけるリンク指定型1対1個別化アクセスチケットPATに対する着信拒否方法について説明する。

【0404】着信拒否の設定：ユーザとセキュア・コミュニケーション・サービスSCS5との間で、任意の手段で双方向認証を行う。次に、ユーザは登録命令とユーザ自身のAIDと任意のPATをSCS5に送信する。次に、SCS5は受信したAIDの署名を検証する。署名が正しくない場合には、SCS5は処理を終了する。署名が正しい場合には、SCS5は受信したすべてのPATについて、それぞれADSの公開鍵を用いて署名を検証する。署名が正しくないPATについては廃棄する。署名が正しい場合には、受信したAIDからリンク情報を取り出し、取り出したリンク情報をそれぞれのPATに提示して検索する。受信したAIDのリンク情報と完全一致するリンク情報を含むPATについては、登録命令とPATを記憶装置に提示して、PATを記憶装置に登録する。受信したAIDのリンク情報と完全一致するリンク情報を含まないPATについては記憶装置に登録せずに廃棄する。なお、上記処理において、ユーザとSCS5間の通信を暗号化する場合もある。

【0405】着信拒否の実行：SCS5はPATを記憶装置に提示して検索する。提示したPATと完全一致するPATが記憶装置に登録されている場合には、メールを廃棄する。提示したPATと完全一致するPATが記憶装置に登録されていない場合には、メールを廃棄しない。

【0406】着信拒否の解除：ユーザとセキュア・コミュニケーション・サービスSCS5との間で、任意の手段で双方向認証を行う。次に、ユーザは自らのAIDをSCS5に提示する。次に、SCS5は受信したAIDの署名を検証する。署名が正しくない場合には、SCS5は処理を終了する。署名が正しい場合には、SCS5は提示されたAIDからリンク情報を取り出し、取り出したリンク情報を検索条件として記憶装置に提示して、

提示されたリンク情報を含むすべてのPATを取得し、ユーザに提示する。次に、ユーザは提示されたすべてのPATを参照し、着信拒否を解除したいPATをすべて選択し、削除命令と併せてSCS5に送信する。削除命令と着信拒否を解除したいすべてのPATを受信したSCS5は、受信した削除命令及びすべてのPATを記憶装置に提示して、受信したすべてのPATを記憶装置から削除する。

【0407】なお、SCSにおけるリンク指定型1対N個別化アクセスチケットPATに対する着信拒否方法も、上記リンク指定型1対1個別化アクセスチケットに対する着信拒否方法と同様である。

【0408】次に、図38のフローチャートおよび図39を参照して、同一性の判定について説明する。

【0409】1. 変数OID_nの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する。また、変数OID_vの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する（ステップS7911）。

【0410】2. 処理対象のリンク情報付きAIDの集合から1個のリンク情報付きAIDを選択し、以下のビット演算を実行する（ステップS7913）。

【0411】(a) リンク情報付きAIDに含まれる位置情報をもとにして、変数AID_nと変数AID_vの値を決定する（ステップS7915）。ここで、

- ・AID_nはOIDの全長Lと等しい長さで、かつ、
- －OID情報が定義されている位置の値は1である。
- －OID情報が定義されていない位置の値は0である。

ビット列と定義する（図39）。

【0412】・AID_vはOIDの全長Lと等しい長さで、かつ、

- －OID情報が定義されている位置の値はOID情報の実際の値である。
- －OID情報が定義されていない位置の値は0である。

ビット列と定義する（図39）。

【0413】(b) OID_nとAID_nのAND演算を実行し、その結果を変数OVR_nに代入する（ステップS7917）。

【0414】(c) OVR_nとAID_nのAND演算と、OVR_nとOID_nのAND演算を実行し、その演算結果を比較する（ステップS7919）。

【0415】・一致する場合OID_nとAID_nのOR演算を実行し、実行結果をOID_nに代入する（ステップS7921）。また、OID_vとAID_vのOR演算を実行し、実行結果をOID_nに代入する（ステップS7923）。

【0416】・一致しない場合、ステップS7925に進み、実行する。

【0417】(d) 処理対象のリンク情報付きAIDの集合から、次に処理するリンク情報付きAIDを抽出す

る。

【0418】・集合に少なくとも1個のリンク情報付きAIDが含まれている場合、ステップS7913-S7923を実行する。

【0419】・集合にリンク情報付きAIDが1個も含まれていない場合、ステップS7927に進む。

【0420】(e) OI_{D_M} およびOI_{D_V} の値を出力する(ステップS7927)。

【0421】最終的に得られたOI_{D_M} の値は、処理対象のリンク情報付きAIDの集合から復元できたOID情報のすべての位置を表している。また、最終的に得られたOI_{D_V} の値は、処理対象のリンク情報付きAIDの集合から復元できたOID情報のすべてを表している。つまり、OI_{D_M} とOI_{D_V} の値を用いると、

(a) OI_{D_V} の値を検索条件とすると、確率的にはあるがOIDを求めることができる。

【0422】(b) 上記検索の精度を、OID全長Lとの比OI_{D_M} / Lで定量的に評価することができる。

【0423】上述したように、本実施形態では、ユーザー要求に基づいて、秘密性かつ信用性の高い第三者機関である認証局CA1において、氏名、電話番号、実Eメールアドレス等秘密性の高い個人情報を含む個人識別子OIDからこれらの個人情報を隠蔽したリンク情報付き役割識別子AIDを生成し、ユーザーに交付する。このAIDを用いて通信網及び通信網上で提供される各種サービスにおいてユーザーを識別することにより、ユーザーの匿名性保証と本人証明の両立が可能になる。つまり、ユーザーは実名や電話番号やEメールアドレスを相手に教えなくても、お互いに通信できるようになるし、後述のように、アノニマス・ディレクトリ・サービスADS7を介して不特定多数に公開情報を開示することもできる。

【0424】ユーザーは、個人情報に比べ秘密性のより低いと思われる情報すなわち公開情報をアノニマス・ディレクトリ・サービスADS7に登録する。公開情報及び登録者AIDを検索する場合には、検索者は検索者のリンク情報付き役割識別子AIDと任意の検索条件をアノニマス・ディレクトリ・サービスADS7に提示する。アノニマス・ディレクトリ・サービスADS7は、すべての検索条件を満足する登録者のリンク情報付き役割識別子AIDを抽出し、次に、検索者のリンク情報付き役割識別子AIDのリンク情報と検索条件を満足した登録者のリンク情報付き役割識別子AIDのリンク情報と移転制御フラグの値と有効期限の値からリンク指定型1対1個別化アクセスチケットPATを生成する。

【0425】このリンク指定型1対1個別化アクセスチケットPATには、図34(c)に示すように、移転制御フラグの値、有効期限の値が設定されるが、この有効期限を事前に設定することにより、発信者からの接続を制限することができる。

【0426】また、移転制御フラグの値により、アクセ

ス権を有していない第三者からの接続を禁止することができる。すなわち、移転制御フラグを1に設定した場合には、セキュア・コミュニケーション・サービスSCS5と発信者との間で任意のチャレンジ/レスポンス方式に従い発信者役割識別子AIDを認証するため、発信者が発信者AIDとPATの両者を発信者以外のいかなるユーザーに渡しても、そのユーザーはアノニマス・ディレクトリ・サービスADS7への登録者にSCS5を介して接続できない。一方、移転制御フラグを0に設定した場合には、SCS5と発信者との間でいかなるチャレンジ/レスポンスも行わないため、発信者が発信者AIDとPATの両者を発信者以外のユーザーに渡したら、それらのユーザーもADS7への登録者にSCS5を介して接続できるようになる。

【0427】また、リンク指定型1対1個別化アクセスチケットPATで着信者を指定した呼をリンク指定型1対1個別化アクセスチケットPATのリンク情報で特定した着信者役割識別子AIDまたは発信者役割識別子AIDに着信するように、通信網に対して接続要求をすることができる。更に、リンク指定型1対1個別化アクセスチケットPATで指定した呼のうち、着信者が選択したリンク指定型1対1個別化アクセスチケットPATの呼を着信拒否することができる。また、着信者が選択したリンク指定型1対1個別化アクセスチケットの呼の着信拒否を解除することもできる。更に、匿名性を悪用し複数の発信者役割識別子AIDで個人攻撃を繰り返す発信者への対処として、それら複数の発信者役割識別子AIDから個人識別子OIDの同一性を判定することができ、かつ、その個人識別子のある確率で取り出すことができる。

【0428】次に、本発明の第7の実施形態に係るメールアクセス制御方法について図40乃至図49を参照して説明する。上述した第6の実施形態では発信者と着信者を1対1に対応させる場合について説明したのに対して、第7の実施形態では、上述した第2の実施形態と同様に、発信者と着信者を1対Nに対応させるとともに、リンク指定型1対N個別化アクセスチケットの新規生成、内容変更をユーザー主導で可能とする場合について説明するものである。なお、この発信者はPATの所有者またはPATの会員のいずれかである。同様に受信者もPATの所有者またはPATの会員のいずれかである。

【0429】第2の実施形態で説明したと同様に、グループ通信(メーリングリスト等)の会員構成は動的に変化するため、グループ通信の主催者は会員の電話番号、電子メールアドレス等の連絡先情報を管理する必要がある。これに対して、第6の実施形態のように、リンク指定型1対1個別化アクセスチケットの新規生成しかできない場合には、連絡先情報の管理が困難である。例えば、グループを一体として管理することが困難であり、また移転制御のため、他の人に渡しても、メーリングリ

スト等グループ通信のアドレスとして機能しない。

【0430】本第7の実施形態では、このような不具合を解消するためにリンク指定型1対N個別化アクセスチケットPATの新規生成および既存のリンク指定型1対N個別化アクセスチケットPATの内容変更をユーザ主導でできるようにしている。

【0431】まず、本第7の実施形態で使用される各識別子の定義について図40、図41を参照して説明する。

【0432】個人識別子OIDは、図40(a)に示すように、認証局CA1がユーザを一意に識別可能な規則に従う任意の文字列と公開鍵から構成される情報に対し認証局CA1が署名したものである。

【0433】リンク情報付き役割識別子AIDは、図40(b)に示すように、個人識別子OIDの断片とその位置情報、冗長な文字列、SCSを動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列(ホスト名、実ドメイン名)であるSCSの情報、およびリンク情報から構成される情報に対し認証局CA1が署名したものである。また、AIDはSCSやCAで暗号化する場合もある。なお、リンク情報は、第6の実施形態のものと同じである。

【0434】リンク指定型1対N個別化アクセスチケット(Personalized Access Ticket: PAT)は、図40(c)に示すように、2個以上の役割識別子のリンク情報、所有者インデックス、有効期限、移転制御フラグ、PAT演算装置識別子から構成される情報に対し、PAT演算装置の秘密鍵により署名したものである。

【0435】ここで、役割識別子AIDのリンク情報の1個は、このPATの所有者役割識別子AIDのリンク情報で、所有者AIDのリンク情報とこれに対応したEnablerをPAT演算装置に提示することにより、PATへのAIDのリンク情報の追加、PATからのAIDのリンク情報の削除、PATの有効期限の変更、PATの移転制御フラグの値の変更等、PATに含まれる情報を変更することができる。

【0436】一方、PATに含まれる所有者AIDのリンク情報以外のAIDのリンク情報はすべて会員AIDのリンク情報で、会員AIDのリンク情報とこれに対応したEnablerをPAT演算装置に提示しても、PATに含まれる情報を変更することはできない。

【0437】所有者インデックスは、所有者AIDのリンク情報を識別するための数値データで、所有者AIDのリンク情報と会員AIDのリンク情報とから構成されるリンク指定型AIDリストにおける先頭のAIDのリンク情報が所有者AIDのリンク情報の場合には1、先頭から2番目のAIDのリンク情報が所有者AIDのリンク情報の場合には2、…、n番目のAIDのリンク情報が所有者AIDのリンク情報の場合にはnであると定義する。

【0438】移転制御フラグは、リンク指定型1対1個別化アクセスチケットの場合と同様、0または1の値をとりうると定義する。

【0439】所有者AIDのリンク情報は、リンク指定型AIDリストにおける所有者インデックスの値の位置に書き込まれているAIDのリンク情報であると定義する。会員AIDのリンク情報は、所有者AIDのリンク情報以外のすべてのAIDのリンク情報と定義する。

【0440】有効期限はPATの使用回数、PATが利用不可能になる絶対時刻(UTC)、PATが利用可能になる絶対時刻(UTC)、PATが利用可能になってから利用不可能になるまでの相対時間(寿命)のいずれか、または複数を組み合わせて定義する。PAT演算装置(またはネットワーク上のPAT演算オブジェクト)の識別子は、PAT演算装置のシリアルナンバー(またはPAT演算オブジェクトのネットワーク上の識別名)であると定義する。

【0441】PAT演算装置(またはネットワーク上のPAT演算オブジェクト)の秘密鍵は、前記識別子に一意に対応すると定義する。

【0442】また、本第7の実施形態では、役割識別子AIDに対応した識別子として、Enablerを導入している。Enablerは、図41に示すように、Enablerであることを一意に表す文字列とリンク情報付きAIDから構成される情報に対して認証局CA1が署名したものである。

【0443】次にPATの新規生成および内容変更における操作について説明する。通信端末上のセキュアなPAT演算装置、CA上もしくはCAから正当に依頼されたネットワーク上のPAT演算オブジェクト(以後、これもPAT演算装置と呼ぶことにする)において、次の操作が定義されるが、これは第2の実施形態のものと同じであり、図10～図13を参照して説明する。

【0444】1. リンク指定型AIDリストの編集
リンク情報付きAIDとEnablerを用いて、PATに含まれるAIDのリンク情報のリストであるリンク指定型AIDリストを編集する。または、リンク指定型AIDリストを新規生成する。

【0445】2. 有効期限及び移転制御フラグの値の設定

リンク情報付きAIDとEnablerを用いて、PATに含まれる有効期限の値および移転制御フラグの値を変更する。または、新たに生成したリンク指定型AIDリストに新たな有効期限の値及び新たな移転制御フラグの値を設定する。

【0446】所有者AIDとこの所有者AIDに対応したEnablerをPAT演算装置に提示したユーザは、PATに含まれるAIDのリンク情報のリストを編集できる。このとき、以下の演算規則に従う。

【0447】(1) 新規生成(MakePAT)(図10参

照) :

リンク指定型AIDリスト (LALIST<(リンク)
所有者AID | (リンク) 会員AID₁, (リンク) 会
員AID₂, ..., (リンク) 会員AID_n>) (但し、
(リンク) AID_x はAID_x のリンク情報であること

を表す) を新規生成し、生成後のLALISTに対し、
有効期限の値および移転制御フラグの値を設定する。

【0448】

【数23】

(リンク) AID_A + (リンク) AID_B
+ Enabler of AID_B + Enabler of AID_A
→ LALIST<(リンク) AID_A | (リンク) AID_B>
LALIST<(リンク) AID_A | (リンク) AID_B>
+ Enabler of AID_A + 有効期限の値 + 移転制御フラグの値
→ PAT<(リンク) AID_A | (リンク) AID_B>

(2) マージ (MergePAT) (図11参照) :

移転制御フラグの値を設定する。

同一所有者AIDの複数LALISTをマージし、マ
ージ後のLALISTに対し、有効期限の値および移転制

【0449】

【数24】

LALIST<(リンク) AID_A | (リンク) AID_{B1},
(リンク) AID_{B2}, ...>
+ LALIST<(リンク) AID_A | (リンク) AID_{C1},
(リンク) AID_{C2}, ...>
+ Enabler of AID_A
→ LALIST<(リンク) AID_A | (リンク) AID_{B1},
(リンク) AID_{B2}, ..., (リンク) AID_{C1},
(リンク) AID_{C2}, ...>
LALIST<(リンク) AID_A | (リンク) AID_{B1},
(リンク) AID_{B2}, ..., (リンク) AID_{C1},
(リンク) AID_{C2}, ...>
+ Enabler of AID_A + 有効期限の値 + 移転制御フラグの値
→ PAT<(リンク) AID_A | (リンク) AID_{B1},
(リンク) AID_{B2}, ..., (リンク) AID_{C1},
(リンク) AID_{C2}, ...>

(3) 分割 (SplitPAT) (図12参照) :

る。

LALISTを同一所有者AIDの複数LALISTに
分解し、分解後のすべてのLALISTに対し、それぞ
れ、有効期限の値および移転制御フラグの値を設定す

【0450】

【数25】

LALIST<(リンク) AID_A | (リンク) AID_{B1},
(リンク) AID_{B2}, ..., (リンク) AID_{C1},
(リンク) AID_{C2}, ...>
+ Enabler of AID_A
→ LALIST<(リンク) AID_A | (リンク) AID_{B1},
(リンク) AID_{B2}, ...>
+ LALIST<(リンク) AID_A | (リンク) AID_{C1},
(リンク) AID_{C2}, ...>
LALIST<(リンク) AID_A | (リンク) AID_{C1},
(リンク) AID_{C2}, ...>
+ Enabler of AID_A + 有効期限の値 + 移転制御フラグの値
→ PAT<(リンク) AID_A | (リンク) AID_{C1},
(リンク) AID_{C2}, ...>

(4) 所有者変更 (TransPAT) (図13参照) :

設定する。

LALISTの所有者AIDを変更し、変更後のLAL
ISTに対し有効期限の値および移転制御フラグの値を

【0451】

【数26】

LALIST<(リンク) AID_A | (リンク) AID_B>

+ LALIST<(リンク)AID_A | (リンク)AID_{C1},
(リンク)AID_{C2}, ...>
+ Enabler of AID_A + Enabler of AID_B
→ LALIST<(リンク)AID_B | (リンク)AID_{C1},
(リンク)AID_{C2}, ...>
LALIST<(リンク)AID_B | (リンク)AID_{C1},
(リンク)AID_{C2}, ...>
+ Enabler of AID_B + 有効期限の値 + 移転制御フラグの値
→ PAT<(リンク)AID_B | (リンク)AID_{C1},
(リンク)AID_{C2}, ...>

有効期限の値の設定における操作では、所有者AIDと 義する。
これに対応したEnabler の両者を所有するユーザにのみ 【0452】
有効期限の値の設定を許可するために、以下の操作を定 【数27】

PAT<(リンク)AID_A | (リンク)AID_B >
+ Enabler of AID_A + 有効期限の値
→ PAT<(リンク)AID_A | (リンク)AID_B >

移転制御フラグの値の設定における操作では、所有者A 下の操作を定義する。
IDとこれに対応したEnabler の両者を所有するユーザ 【0453】
にのみ移転制御フラグの値の設定を許可するために、以 【数28】

PAT<(リンク)AID_A | (リンク)AID_B >
+ Enabler of AID_A + 移転制御フラグの値
→ PAT<(リンク)AID_A | (リンク)AID_B >

次に、本実施形態の全体構成を示す図42～図48につ
いて説明する。図42～図48において、CAからAID_A
を割り当てられたユーザAは、ユーザAの計算機に
AID_A および Enabler of AID_A を保存し、フロッ
ピードライブ、CD-ROMドライブ、通信ボード、マ
イクロフォン、スピーカー等の入出力機器を接続してい
る。または、記憶装置及びデータ入出力機能を備える通
信端末（電話、携帯電話等）に、AID_A および Enabl
er of AID_A を保存している。

【0454】同様に、CAからAID_B を割り当てられ
たユーザBは、自らの計算機にAID_B および Enabler
of AID_B を保存し、フロッピードライブ、CD-R
OMドライブ、通信ボード、マイクroフォン、スピーカ
ー等の入出力機器を接続している。または、記憶装置及
びデータ入出力機能を備える通信端末（電話、携帯電話
等）に、AID_B および Enabler of AID_B を保存し
ている。

【0455】以下、ユーザAがPAT<(リンク)AID_A
| (リンク)AID_B >を生成する手順を説明す
る。

【0456】(1) ユーザAは、以下の手段のいずれかを
用いて、AID_B および Enabler of AID_B を取得す
る。

【0457】・アノニマス・ディレクトリ・サービスA
DS7にAID_B と Enabler of AID_B を登録し、ユ
ーザAが検索結果として取得するのを待つ（図42）。

【0458】・電子メール、シグナリング等でAID_B
と Enabler of AID_B をユーザAに直接送信する（図

43～図44）。

【0459】・フロッピーディスク、CD-ROM、M
O、ICカード等の磁気、光、電子メディアにAID_B
と Enabler of AID_B を蓄積し、ユーザAに渡す。ま
たは、ユーザAが閲覧して取得するのを待つ（図45～
図46）。

【0460】・書籍、名刺等の紙メディアにAID_B と
Enabler of AID_B を記載し、ユーザAに渡す。もし
くは、ユーザAが閲覧し取得するのを待つ（図47～図
48）。

【0461】(2) 上述した(1)のいずれかの手段でA
ID_B および Enabler of AID_Bを取得したユーザA
は、PAT演算装置に対しMakePAT命令を発行する。
この手順は図42～図48で共通で、以下の通りに定義
する。

【0462】(a) ユーザAは、ユーザAの通信端末にA
ID_A、Enabler of AID_A、AID_B、Enabler o
f AID_B、有効期限の値、および移転制御フラグの値
をセットし、MakePAT命令の発行を要求する。

【0463】(b) ユーザAの通信端末は、MakePAT命
令を生成する。

【0464】(c) ユーザAの通信端末は、生成したMake
PAT命令を電子メール、シグナリング等の手段でPA
T演算装置に送信する（MakePAT命令の発行）。

【0465】(d) PAT演算装置は、受信したMakePA
T命令を図21、図49に従って処理し、PAT<(リ
ンク)AID_A | (リンク)AID_B >を生成する。具
体的には、

【数29】

(リンク) AID_A + (リンク) AID_B
 + Enabler of AID_B + Enabler of AID_A
 → LALIST<(リンク) AID_A | (リンク) AID_B >
 LALIST<(リンク) AID_A | (リンク) AID_B >
 + Enabler of AID_A + 有効期限の値 + 移転制御フラグの値
 → PAT<(リンク) AID_A | (リンク) AID_B >

(e) PAT演算装置は、生成したPAT<(リンク) AID_A | (リンク) AID_B >を電子メール、シグナリング等の手段でユーザAの通信端末、または必要に応じて、ユーザBの通信端末に送信する。

【0466】(f) ユーザA(またはユーザB)の通信端末は、受信したPAT<(リンク) AID_A | (リンク) AID_B >をユーザAの通信端末の記憶装置に保存する。

【0467】PATのマージ(MergePAT、図21、図49)、PATの分割(SplitPAT、図22、図49)、PATの所有者変更(TransPAT、図21、図49)も同様の手順である。

【0468】MakePAT、MergePAT、TransPATの手順については、AIDをAIDのリンク情報に置き換えAIDリストをリンク指定型AIDリストに置き換える以外は図21を参照して前述した通りである。また、SplitPATの手順についても、AIDをAIDのリンク情報に置き換えAIDリストをリンク指定型AIDリストに置き換える以外は図22を参照して前述したとおりである。

【0469】但し、図21、図22の手順において、リンク指定型AIDリストの生成は、図49のフローチャートにより次のように行う。すなわち、まずバッファ長を決定し(ステップS9011)、バッファを生成する(ステップS9012)。次いで、所有者AIDのリンク情報を生成したバッファの空き領域にコピーする(ステップS9017)。次いで、会員AIDのリンク情報をバッファの空き領域にコピーし(ステップS9018)、次の会員AIDが存在すれば(ステップS9015YES)ステップS9018を繰り返す。

【0470】次に、所有者AIDのリンク情報の決定について説明する。

【0471】MakePAT、MergePAT、SplitPAT、TransPATの各命令は、2個以上の引数を持ち、引数として、役割識別子AID、個別化アクセスチケットPAT、または、Enablerを指定できると定義する。このとき、PAT演算装置は、各命令実行後に出力されるPATの所有者AIDのリンク情報をそれぞれ下記の規則に従い指定する。

SplitPAT PAT₁ (AID₁₁) (AID₂₁ AID₂₂) …
 (AID_{N1} AID_{N2} … AID_{NM}) Enabler of AID

—PAT演算装置は、SplitPAT命令の第1引数のPATの所有者AIDのリンク情報を、SplitPAT命令

【0472】・MakePATの場合

MakePAT命令に対して、第1引数から第N引数(N=2, 3, …)までAIDを、第N+1引数以降ではEnablerを指定すると定義する。例えば、

MakePAT AID₁ AID₂ … AID_N Enabler of AID₁

Enabler of AID₂ … Enabler of AID_N

—PAT演算装置は、MakePAT命令の第1引数のAIDのリンク情報を所有者AIDのリンク情報であると解釈する。

【0473】—第N+1引数以降のEnablerのいずれかが第1引数のAIDに対応している場合に限り、PAT演算装置はこのAIDのリンク情報(すなわち、第1引数のAIDのリンク情報)をMakePAT命令実行後に出力されるPATの所有者AIDのリンク情報に指定する。

【0474】・MergePATの場合

MergePAT命令に対して、第1引数から第N引数(N=2, 3, …)までPATを、第N+1引数ではEnablerを指定すると定義する。すなわち、

MergePAT PAT₁ PAT₂ … PAT_N Enabler of AID

—PAT演算装置は、MergePAT命令の第1引数のPATの所有者AIDのリンク情報を、MergePAT命令実行後に出力されるPATの所有者AIDのリンク情報であると解釈する。

【0475】—第N+1引数のEnablerが第1引数のPATの所有者AIDに対応している場合に限り、PAT演算装置はこのAIDのリンク情報(すなわち、第1引数のPATの所有者AIDのリンク情報)をMergePAT命令実行後に出力されるPATの所有者AIDのリンク情報に指定する。

【0476】・SplitPATの場合

SplitPAT命令に対して、第1引数でPATを、第2引数から第N引数(N=3, 4, …)まではあらかじめ定められた何らかの記号(この例ではカッコ())とする)でまとめられた1個以上のAIDのまとまりを、第N+1引数ではEnablerを指定すると定義する。すなわち、

SplitPAT PAT₁ (AID₁₁) (AID₂₁ AID₂₂) …
 (AID_{N1} AID_{N2} … AID_{NM}) Enabler of AID
 実行後に出力されるPATの所有者AIDのリンク情報であると解釈する。

【0477】-第N+1引数のEnabler が第1引数のPATの所有者AIDに対応している場合に限り、PAT演算装置はこのAIDのリンク情報(すなわち、第1引数のPATの所有者AIDのリンク情報)をSplitPAT命令実行後に出力されるPATの所有者AIDのリン

TransPAT PAT₁ PAT₂ AID

Enabler of AID₁ Enabler of AID₂

-PAT演算装置は、TransPAT命令の第3引数のAIDのリンク情報が第2引数のPATに含まれている場合に限り、第3引数のAIDのリンク情報を、TransPAT命令実行後に出力されるPATの所有者AIDのリンク情報であると解釈する。

【0479】-第4引数のEnabler が第1引数のPAT及び第2引数のPATの両者に対応しており、かつ、第5引数のEnabler が第3引数のAIDに対応している場合に限り、PAT演算装置は第3引数のAIDのリンク情報をTransPAT命令実行後に出力されるPATの所有者AIDのリンク情報に指定する。

【0480】次に、会員AIDのリンク情報の決定について説明する。MakePAT, MergePAT, SplitPAT, TransPAT各命令の定義は上記に従う。PAT演算装置は、各命令実行後に出力されるPATの会員AIDのリンク情報をそれぞれ下記の規則に従い指定する。

【0481】・MakePATの場合

MakePAT命令実行後に出力されるPATの所有者AIDのリンク情報が正式に決定された場合に限り、

-PAT演算装置は、MakePAT命令の第2引数以降のすべてのAIDのリンク情報をMakePAT命令実行後に出力されるPATの会員AIDのリンク情報であると解

SplitPAT PAT (AID₁₁) (AID₂₁ AID₂₂) …

(AID_{N1} AID_{N2} … AID_{NM}) Enabler of AID

の場合、(AID₁₁)と(AID₂₁ AID₂₂)と(AID_{N1} AID_{N2} … AID_{NM})のリンク情報は所有者AIDのリンク情報が共通な別のPATの会員AIDのリンク情報になる。

【0485】・TransPATの場合

PAT演算装置は、TransPAT命令実行後に出力されるPATの所有者AIDのリンク情報が正式に決定された場合に限り、TransPAT命令の第1引数で指定されたPATのすべての会員AIDのリンク情報及び第2引数で指定されたPATの会員AIDのリンク情報のうち新所有者となる予定の会員AIDのリンク情報を除いた残りのすべての会員AIDのリンク情報を、TransPAT命令実行後に出力されるPATの会員AIDのリンク情報に指定する。

【0486】本実施形態の、Enabler の正当性の検証は図24を参照した前述した説明と同じである。また、このEnabler の正当性の検証は、MakePAT, MergePAT, SplitPAT, TransPATで共通である。

【0487】次に、本発明の第8の実施形態について説

ク情報に指定する。

【0478】・TransPATの場合

TransPAT命令に対して、第1引数及び第2引数でPATを、第3引数でAIDを、第4引数及び第5引数ではEnablerを指定すると定義する。すなわち、

積する。

【0482】-第2引数以降のすべてのAIDのうち、第N+1引数以降で指定されたEnabler と対応しているAIDのリンク情報のみ、PAT演算装置はMakePAT命令実行後に出力されるPATの会員AIDのリンク情報に指定する。

【0483】・MergePATの場合

PAT演算装置は、MergePAT命令実行後に出力されるPATの所有者AIDのリンク情報が正式に決定された場合に限り、MergePAT命令の第1引数から第N引数で指定されたすべてのPATの会員AIDのリンク情報を、MergePAT命令実行後に出力されるPATの会員AIDのリンク情報に指定する。

【0484】・SplitPATの場合

PAT演算装置は、SplitPAT命令実行後に出力されるPATの所有者AIDのリンク情報が正式に決定された場合に限り、SplitPAT命令の第1引数で指定されたPATの会員AIDのリンク情報を、SplitPAT命令実行後に出力されるPATの会員AIDのリンク情報に指定する。このとき、会員AIDのリンク情報はカッコ()単位で別々のPATに振り分けられる。例えば、

明する。

【0488】本第8の実施形態においては、個人識別子OIDは実メールアドレスである。個別化アクセスチケットPATは2個以上の実メールアドレス、所有者インデックス、有効期限、移転制御フラグ、及び、PAT演算装置(またはネットワーク上のPAT演算オブジェクト)の識別子から構成される情報に対して、PAT演算装置(またはネットワーク上のPAT演算オブジェクト)の秘密鍵で署名したものである。

【0489】実メールアドレスのうち、1個はこのPATの所有者メールアドレスで、所有者メールアドレスと所有者メールアドレスを含むEnabler の両者をPAT演算装置(またはネットワーク上のPAT演算オブジェクト)に提示することにより、PATへの実メールアドレスの追加、削除、PATの有効期限の変更、PATの移転制御フラグの値の変更など、PATに含まれる情報を変更することができる。

【0490】一方、PATに含まれる実メールアドレスのうち、所有者メールアドレス以外の実メールアドレス

はすべて会員メールアドレスで、会員メールアドレスと会員メールアドレスを含むEnabler をPAT演算装置（またはネットワーク上のPAT演算オブジェクト）に提示しても、PATに含まれる情報を変更することはできない。

【0491】所有者インデックスは、所有者メールアドレスを識別するための数値データである。所有者メールアドレスと会員メールアドレスから構成されるメールアドレスリストにおいて、先頭の実メールアドレスが所有者メールアドレスの場合には1、先頭から2番目の場合には2、…、n番目の場合にはnであると定義する。

【0492】メールアドレスリストにおいて、所有者メールアドレスは所有者インデックスで指定された位置に書き込まれている実メールアドレスと定義する。一方、会員メールアドレスは、所有者メールアドレス以外のすべての実メールアドレスであると定義する。

【0493】移転制御フラグは0または1の値をとると定義する。

【0494】有効期限はPATの使用回数、PATが利用不可能になる絶対時刻（UTC）、PATが利用可能になる絶対時刻（UTC）、PATが利用可能になってから利用不可能になるまでの相対時間（寿命）のいずれか、または複数を組み合わせて定義する。

【0495】PAT演算装置（またはネットワーク上のPAT演算オブジェクト）の識別子は、PAT演算装置のシリアルナンバー（またはPAT演算オブジェクトのネットワーク上の識別名）であると定義する。

【0496】PAT演算装置（またはネットワーク上のPAT演算オブジェクト）の秘密鍵は、前記識別子に一意に対応すると定義する。

【0497】また、実メールアドレスに対応した識別子として、Enablerを定義する。Enablerは、Enablerであることを一意にあらわす情報と実メールアドレスから構成されるデータに対して、PAT演算装置（またはネットワーク上のPAT演算オブジェクト）の秘密鍵で署名したものである。

【0498】PATの生成は以下に行う。

【0499】ネットワーク上のPAT演算オブジェクトの一例として、ディレクトリを挙げる。ディレクトリはユーザの実メールアドレスと公開情報を対応づけて管理し、任意のユーザから提示された検索条件を入力し、PATを出力する。

【0500】ユーザは実メールアドレスと検索条件をディレクトリに送信する。ディレクトリは検索条件を満足する公開情報と一意に対応した実メールアドレスをすべて取得する。次に、検索条件を提示したユーザの実メールアドレスと、検索結果として取得したすべての実メールアドレスから実メールアドレスのリストを構成する。次に、所有者インデックスの値、有効期限の値、転移制御フラグの値、及び、ディレクトリの識別名を追加す

る。最後に、これらをすべて追加したデータに対しディレクトリの秘密鍵で署名してPATとして、検索条件を提示したユーザに送信する。

【0501】メールアクセス制御は以下に行う。

【0502】発信者はメールのFrom：行に送信者の実メールアドレスを、To：行にPAT@発信者の実ドメインを指定する。

【0503】SCSはSMTP (Simple Mail Transfer Protocol) 等のMTA (Message Transfer Agent) への着信メールを取得し、以下の手順に従い認証する。

【0504】1. PATの署名をPATの公開鍵を用いて検証する。

【0505】・PATに改竄が認められる場合には、メールを廃棄して終了する。

【0506】・PATに改竄が認められない場合には、下記処理2. を実行する。

【0507】2. 発信者の実メールアドレスをPATに提示して検索する。

【0508】・発信者の実メールアドレスと完全一致する実メールアドレスがPATに含まれていない場合には、メールを廃棄して終了する。

【0509】・発信者の実メールアドレスと完全一致する実メールアドレスがPATに含まれている場合には、下記処理3. を実行する。

【0510】3. PATの有効期限を評価する。

【0511】・PATが有効期限外の場合には、メールを廃棄して終了する。

【0512】・PATが有効期限内の場合には、下記処理4. を実行する。

【0513】4. PATの移転制御フラグの値を参照して、発信者を認証するか否かを決定する。

【0514】・値が1の場合には、SCSと発信者との間でチャレンジ/レスポンス認証を実行して、発信者の署名を検証する。署名が正しい場合には、着信者を指定し、PATを添付する。署名が正しくない場合には、メールを廃棄して終了する。

【0515】・値が0の場合には、チャレンジ/レスポンス認証を実行せずに、着信者を指定し、チケットを添付する。

【0516】SCSと発信者との間のチャレンジ/レスポンスの例を説明する。

【0517】まず、SCSは任意の情報、例えばタイムスタンプを生成し、生成した情報を発信者に任意の手段で送信する。

【0518】次に、発信者は秘密鍵と公開鍵を生成し、受信した情報に秘密鍵で署名し、公開鍵とあわせてSCSに任意の手段で送信する。

【0519】最後に、SCSは、受信した情報の署名を発信者から提示された公開鍵を用いて検証する。署名が正しい場合には、着信者を指定し、PATを添付する。

署名が正しくない場合にはメールを廃棄して終了する。

【0520】着信者の指定及びチケットの添付は以下のように行う。

【0521】SCSは、まず、発信者の実メールアドレスをPATに提示して検索し、発信者の実メールアドレスと完全一致しないすべての実メールアドレスを取得する。次に、取得したすべての実メールアドレスを着信者の実メールアドレスに指定する。

【0522】次に、SCSは、双方向通信を可能とすべく、PATをすべて着信者メールアドレスに送信するために、PATをメールの任意の箇所に添付する。

【0523】最後に、SCSはMTAにメールを渡す。

【0524】着信拒否は以下のように行う。

【0525】着信拒否の設定：ユーザとセキュア・コミュニケーション・サービスSCS5との間で、任意の手段で双方向認証を行う。次に、ユーザは登録命令とユーザ自身の実メールアドレスと任意のPATをSCS5に送信する。次に、SCS5は受信したすべてのPATについて、それぞれADSの公開鍵を用いて署名を検証する。署名が正しくないPATについては廃棄する。署名が正しい場合には、受信した実メールアドレスをそれぞれのPATに提示して検索する。受信した実メールアドレスと完全一致する実メールアドレスを含むPATについては、登録命令とPATを記憶装置に提示して、PATを記憶装置に登録する。受信した実メールアドレスと完全一致する実メールアドレスを含まないPATについては記憶装置に登録せずに廃棄する。

【0526】着信拒否の実行：SCS5はPATを記憶装置に提示して検索する。提示したPATと完全一致するPATが記憶装置に登録されている場合には、メールを廃棄する。提示したPATと完全一致するPATが記憶装置に登録されていない場合には、メールを廃棄しない。

【0527】着信拒否の解除：ユーザとセキュア・コミュニケーション・サービスSCS5との間で、任意の手段で双方向認証を行う。次に、ユーザは自らの実メールアドレスをSCS5に提示する。次に、SCS5は提示された実メールアドレスを検索条件として記憶装置に提示して、提示された実メールアドレスを含むすべてのPATを取得し、ユーザに提示する。次に、ユーザは提示されたすべてのPATを参照し、着信拒否を解除したいPATをすべて選択し、削除命令と併せてSCS5に送信する。削除命令と着信拒否を解除したいすべてのPATを受信したSCS5は、受信した削除命令及びすべてのPATを記憶装置に提示して、受信したすべてのPATを記憶装置から削除する。

【0528】PATの編集は以下のように行う。

【0529】役割識別子AIDを要素とするPATに対するMakePAT、MergePAT、SplitPAT、TransPAT演算において、役割識別子AIDを実メールアドレス

に、役割識別子AIDに対するEnablerを実メールアドレスに対するEnablerにそれぞれ置き換えると、実メールアドレスを要素とするPATに対するMakePAT、MergePAT、SplitPAT、TransPAT演算になる。

【0530】Null演算子はNullであることを一意に表し、かつ、実メールアドレスの形式を持つ情報から構成される情報に対し、PAT演算装置またはネットワーク上のPAT演算オブジェクトの秘密鍵で署名したものである。

【0531】同様に、God演算子はGodであることを一意に表し、かつ、実メールアドレスの形式を持つ情報から構成される情報に対し、PAT演算装置またはネットワーク上のPAT演算オブジェクトの秘密鍵で署名したものである。

【0532】Null演算子のEnablerはEnablerであることを一意に表す情報とNull演算子の実体から構成される情報に対し、PAT演算装置またはネットワーク上のPAT演算オブジェクトの秘密鍵で署名したものである。

【0533】Null演算子及びGod演算子を用いた演算は、役割識別子AIDを要素とするPATに対するすべての演算において、役割識別子AIDを実メールアドレスに、役割識別子AIDに対するEnablerを実メールアドレスに対するEnablerに置き換えることで求められる。さらに、Null-AIDをNull演算子に、God-AIDをGod演算子に、また、Null-AIDに対するEnablerをNull演算子に対するEnablerに置き換えることで求められる。

【0534】

【発明の効果】以上説明したように、本発明によれば、個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間のメールアクセス制御を行うので、ユーザの本当の識別子を隠蔽しつつ、ユーザの特性を表す情報を公開し、この情報に基づいて適切な通信を行うことができ、第三者からの攻撃等を防止することができる。加えて、着信者が匿名性を悪用した発信者による攻撃を受けた場合には、その攻撃による着信者への被害を最小限に食い止めることができる。

【0535】また、本発明によれば、個別化アクセスチケットの新規生成、内容変更を各ユーザに付与された役割識別子AIDとこのAIDに対応して定義されたEnablerを用いてユーザ主導で行うことができるので、例えば動的に変化するグループ通信（メーリングリスト等）の会員の連絡先情報等も適確に管理することができる。

【0536】更に、本発明によれば、Null-AIDとNull-AIDのEnablerを導入して、会員AIDおよびEnabler of 会員AIDを個別化アクセスチケットPATの所有者に渡さなくてもPATの新規生成（MakePAT）および所有者変更（TransPAT）を行うことができるので、会員AIDを用いた成りすましを防止

することができる。

【0537】本発明によれば、Null-AIDは個別化アクセスチケットPATの所有者AIDとしてのみ使用可能（Null-AIDはPATの会員AIDには使用不可能）であり、 $PAT < AID_{Null} | AID_{member1}, AID_{member2}, \dots, AID_{memberN} >$ は許可するが $PAT < AID_{holder} | AID_{Null}, AID_{member1}, AID_{member2}, \dots, AID_{memberN} >$ は許可しないので、 $PAT < AID_{holder} | AID_{member} >$ の所有者が AID_{member} のEnablerを知らない限り、この $PAT < AID_{holder} | AID_{member} >$ から $PAT < AID_{Null} | AID_{member} >$ を作成することはできない。

【0538】また、本発明によれば、God-AIDを導入して、個別化アクセスチケットPATに読取専用属性を設定できるので、グループ通信において参加者を固定することができる。

【0539】更に、本発明によれば、役割識別子を一意に特定するためのリンク情報を導入して、個別化アクセスチケットPATをリンク情報により定義してPATには役割識別子の実体を含まないようにできるため、役割識別子の実体を使用することなく着信拒否機能を実現することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態の全体構成図。

【図2】第1の実施形態に使用される個人識別子OIDと役割識別子AIDと個別化アクセスチケットPATのデータ構造を示す図。

【図3】第1の実施形態での認証局CAにおける役割識別子AIDの生成処理を示すフローチャート。

【図4】第1の実施形態でのアノニマス・ディレクトリ・サービスADSにおける個別化アクセスチケットPATの生成処理を示すフローチャート。

【図5】第1の実施形態でのセキュア・コミュニケーション・サービスSCSにおけるメール転送制御を示すフローチャート。

【図6】第1の実施形態でのセキュア・コミュニケーション・サービスSCSにおける役割識別子AIDの同一性判定処理を示すフローチャート。

【図7】図6に示す同一性判定処理に用いるデータの例を示す図。

【図8】本発明の第2の実施形態に使用される個人識別子OIDと役割識別子AIDと個別化アクセスチケットPATのデータ構造を示す図。

【図9】本発明の第2の実施形態に使用される役割識別子AIDとEnablerのデータ構造を示す図。

【図10】本発明の第2の実施形態に使用される演算規則（MakePAT）の定義を示す図。

【図11】本発明の第2の実施形態に使用される演算規則（MergePAT）の定義を示す図。

【図12】本発明の第2の実施形態に使用される演算規則（SplitPAT）の定義を示す図。

【図13】本発明の第2の実施形態に使用される演算規則（TransPAT）の定義を示す図。

【図14】本発明の第2の実施形態におけるシステム構成（1）を示す図。

【図15】本発明の第2の実施形態におけるシステム構成（2）を示す図。

【図16】本発明の第2の実施形態におけるシステム構成（3）を示す図。

【図17】本発明の第2の実施形態におけるシステム構成（4）を示す図。

【図18】本発明の第2の実施形態におけるシステム構成（5）を示す図。

【図19】本発明の第2の実施形態におけるシステム構成（6）を示す図。

【図20】本発明の第2の実施形態におけるシステム構成（7）を示す図。

【図21】本発明の第2の実施形態での演算処理（MakePAT, MergePAT, TransPAT）の流れを示すフローチャート。

【図22】本発明の第2の実施形態での演算処理（SplitPAT）の流れを示すフローチャート。

【図23】本発明の第2の実施形態におけるAIDリストの生成処理（MakePAT, MergePAT, SplitPAT, TransPAT）を示すフローチャート。

【図24】本発明の第2の実施形態におけるEnablerの正当性の検証処理（MakePAT, MergePAT, SplitPAT, TransPAT）を示すフローチャート。

【図25】本発明の第3の実施形態に使用されるNull-AIDのデータ構造を示す図。

【図26】本発明の第3の実施形態に使用されるEnabler of Null-AIDのデータ構造を示す図。

【図27】本発明の第3の実施形態の第1の応用例を示す図。

【図28】本発明の第3の実施形態の第2の応用例を示す図。

【図29】本発明の第4の実施形態に使用されるGod-AIDのデータ構造を示す図。

【図30】本発明の第4の実施形態の第1の応用例を示す図。

【図31】本発明の第4の実施形態の第2の応用例を示す図。

【図32】本発明の第5の実施形態における会員AIDのチェック処理を示すフローチャート。

【図33】本発明の第6の実施形態の全体構成図。

【図34】第6の実施形態に使用される個人識別子OID、リンク情報付き役割識別子AID、リンク指定型1対1個別化アクセスチケットPATのデータ構造を示す図。

【図35】第6の実施形態での認証局CAにおけるリンク情報付き役割識別子AIDの生成処理を示すフローチャート。

【図36】第6の実施形態でのアノニマス・ディレクトリ・サービスADSにおけるリンク指定型1対1個別化アクセスチケットPATの生成処理を示すフローチャート。

【図37】第6の実施形態でのセキュア・コミュニケーション・サービスSCSにおけるメール転送制御を示すフローチャート。

【図38】第6の実施形態でのセキュア・コミュニケーション・サービスSCSにおけるリンク情報付き役割識別子AIDの同一性判定処理を示すフローチャート。

【図39】図38に示す同一性判定処理に用いるデータの例を示す図。

【図40】本発明の第7の実施形態に使用される個人識別子OID、リンク情報付き役割識別子AID、リンク指定型1対N個別化アクセスチケットPATのデータ構造を示す図。

【図41】本発明の第7の実施形態に使用されるリンク情報付き役割識別子AIDとEnablerのデータ構造を示す図。

【図42】本発明の第7の実施形態におけるシステム構

成(1)を示す図。

【図43】本発明の第7の実施形態におけるシステム構成(2)を示す図。

【図44】本発明の第7の実施形態におけるシステム構成(3)を示す図。

【図45】本発明の第7の実施形態におけるシステム構成(4)を示す図。

【図46】本発明の第7の実施形態におけるシステム構成(5)を示す図。

【図47】本発明の第7の実施形態におけるシステム構成(6)を示す図。

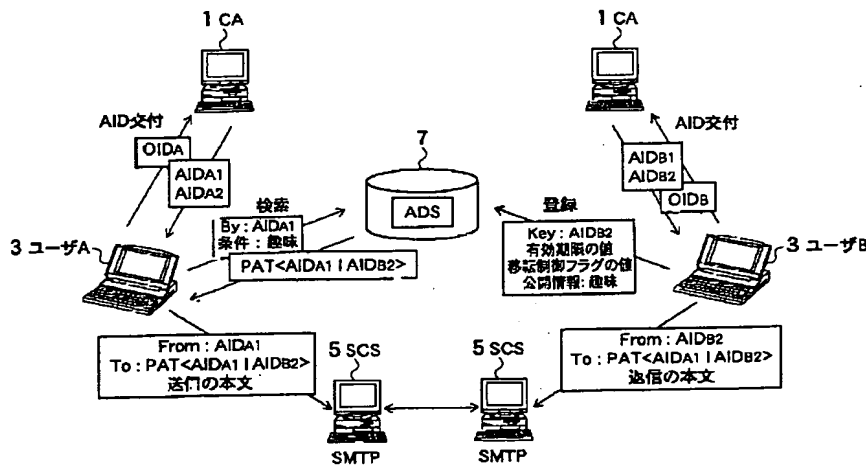
【図48】本発明の第7の実施形態におけるシステム構成(7)を示す図。

【図49】本発明の第7の実施形態におけるリンク指定型AIDリストの生成処理(MakePAT, MergePAT, SplitPAT, TransPAT)を示すフローチャート。

【符号の説明】

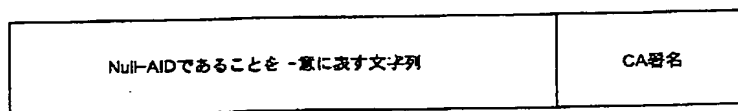
- 1 認証局CA
- 3 ユーザ
- 5 セキュア・コミュニケーション・サービスSCS
- 7 アノニマス・ディレクトリ・サービスADS

【図1】

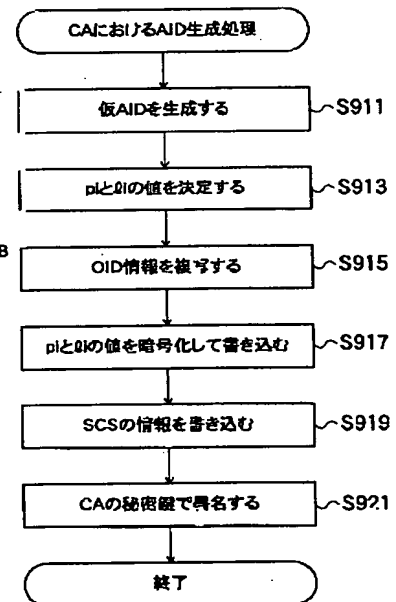


【図25】

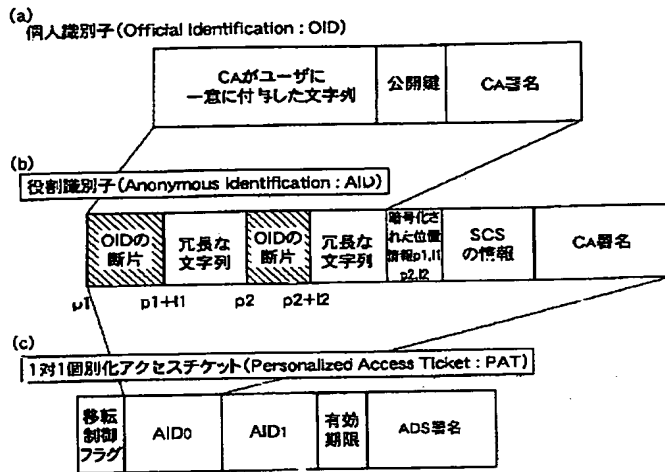
Null-AIDのデータ構造



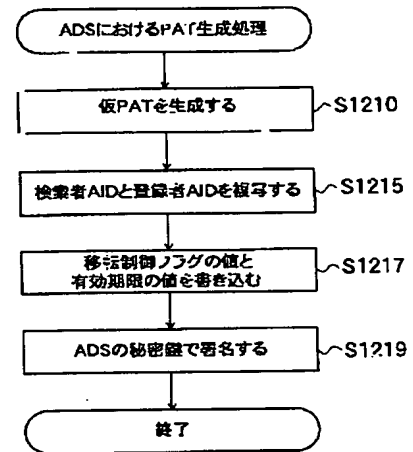
【図3】



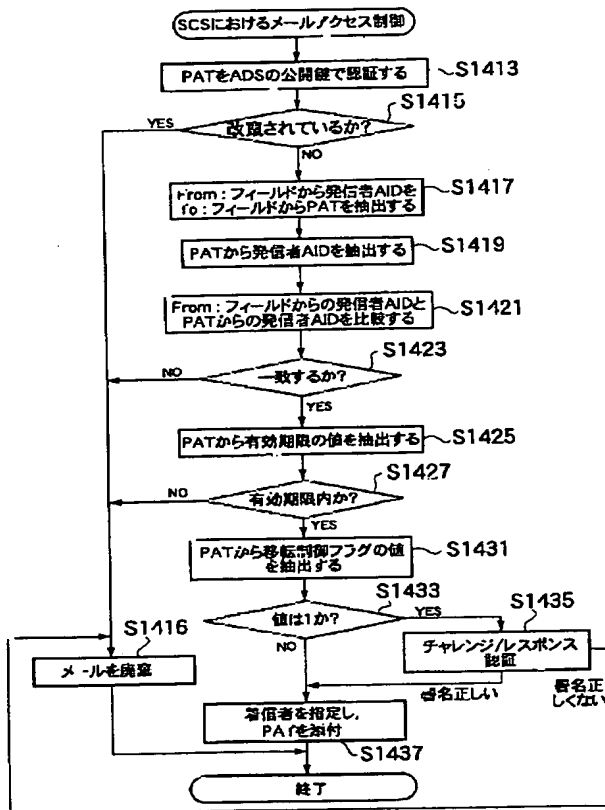
【図2】



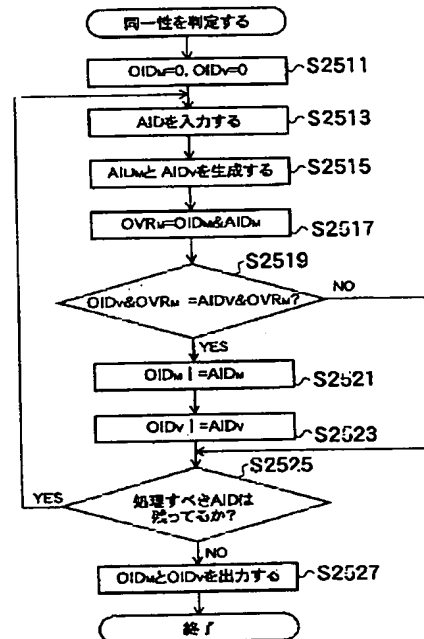
【図4】



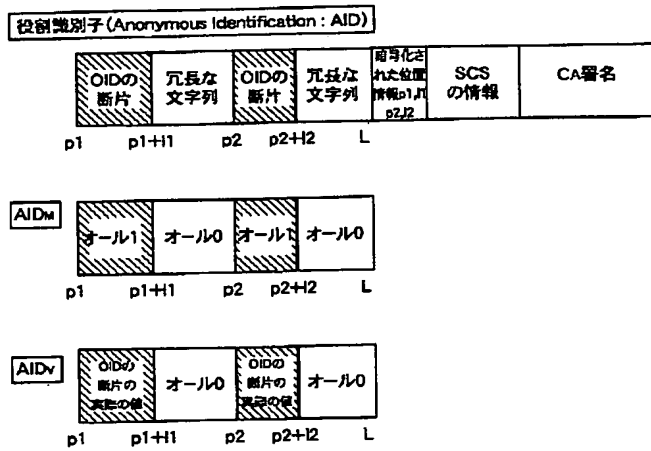
【図5】



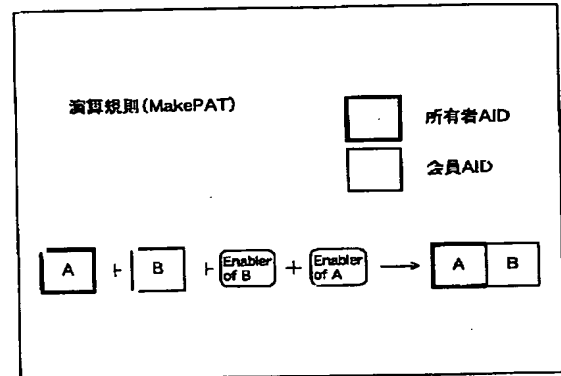
【図6】



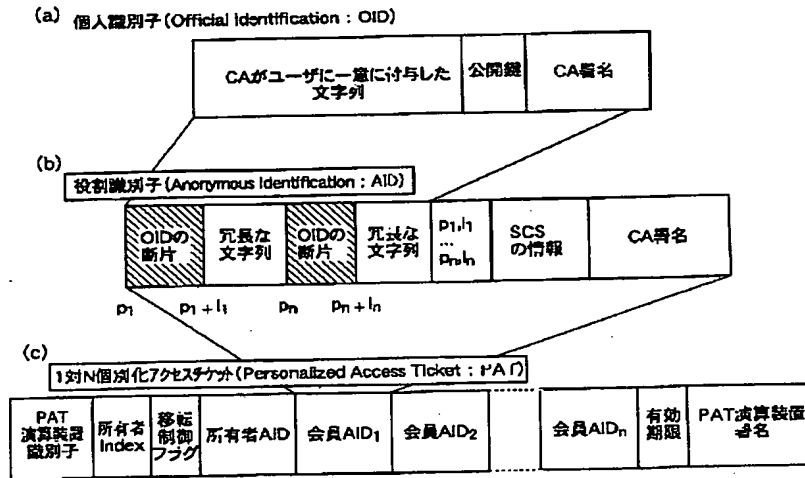
【図7】



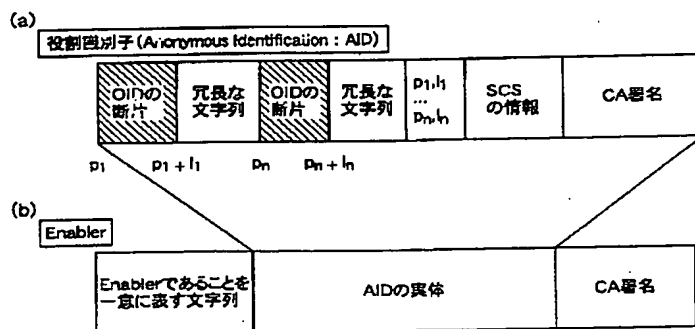
【図10】



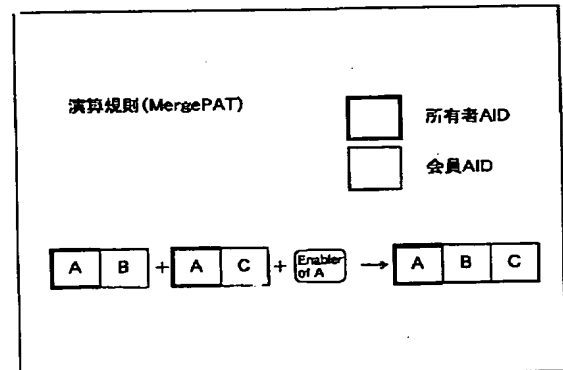
【図8】



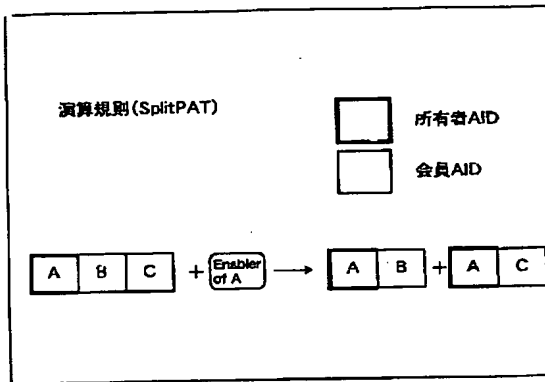
【図9】



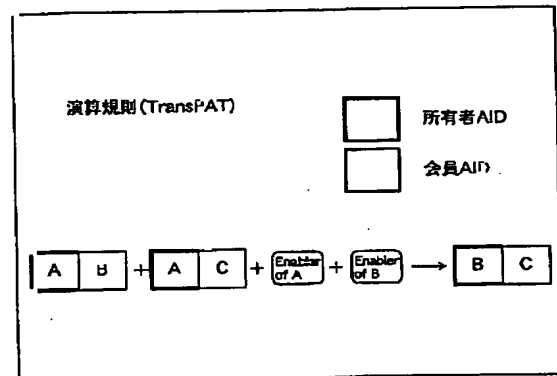
【図11】



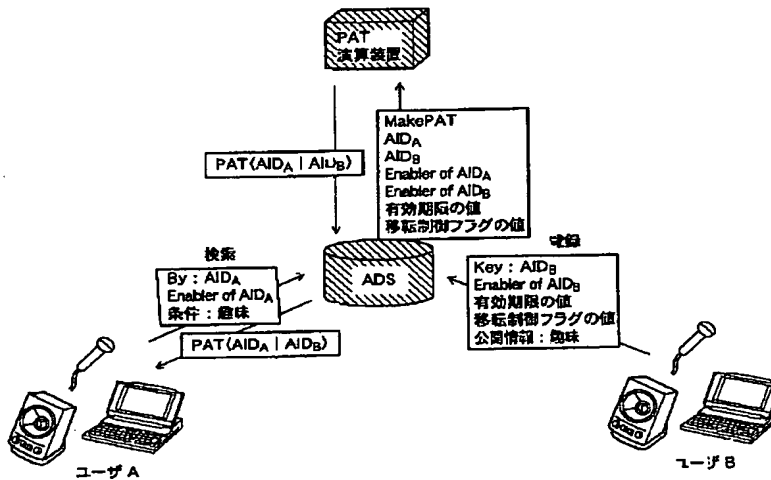
【図12】



【図13】

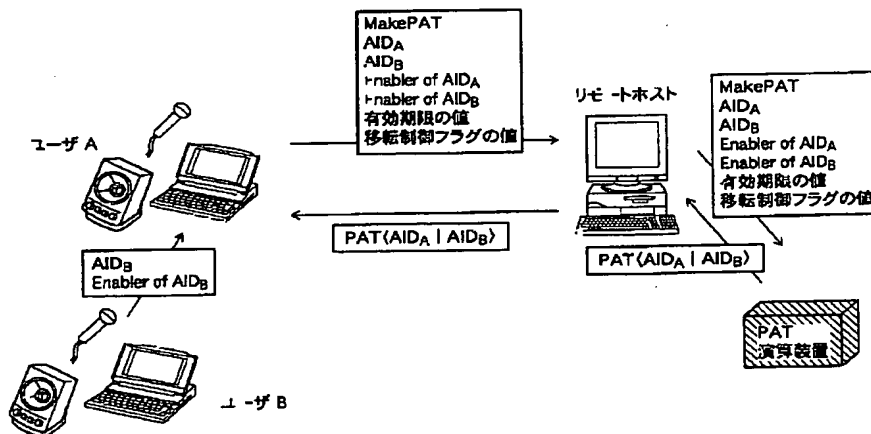


【図14】



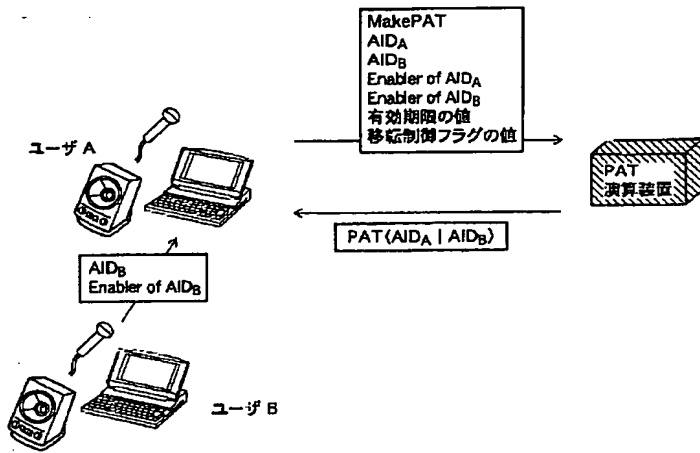
システム構成(1)

【図16】



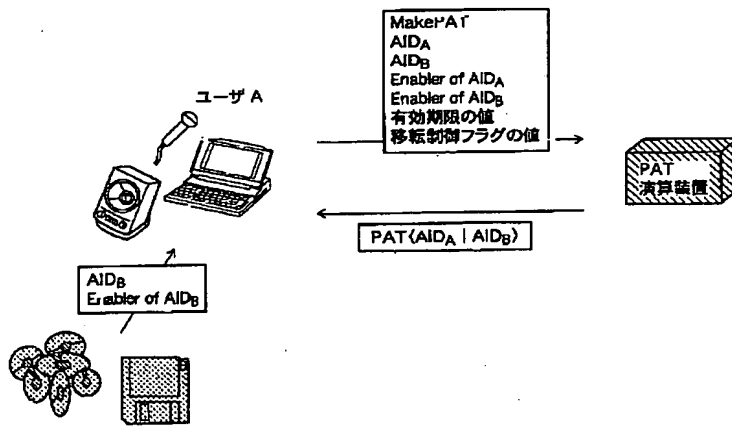
システム構成(3)

【図15】



システム構成(2)

【図17】



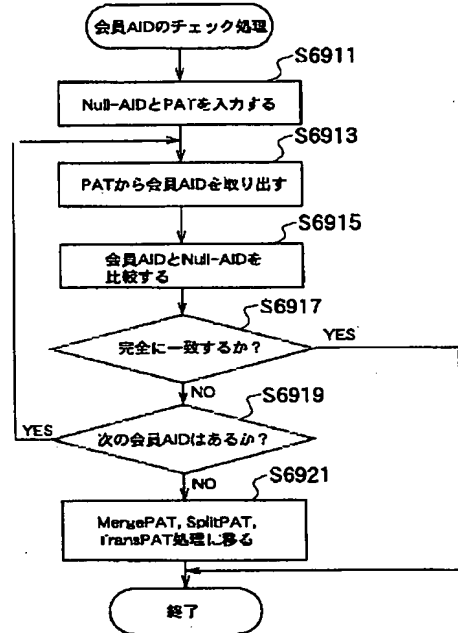
システム構成(4)

【図26】

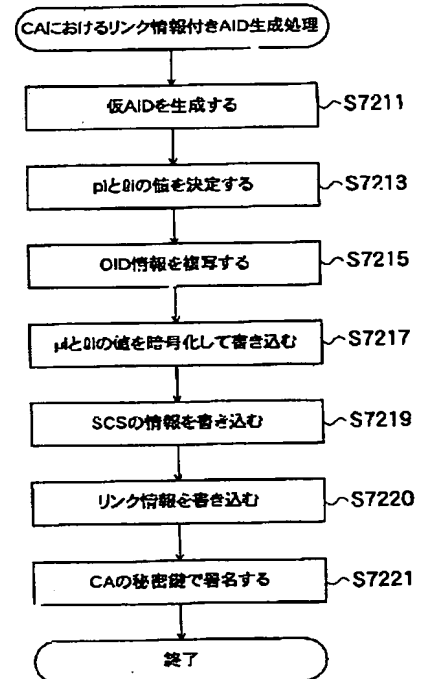
Enabler of Null-AIDのデータ構造

Enablerであることを一意に表す文字列	Null-AIDの実体	CA署名
-----------------------	-------------	------

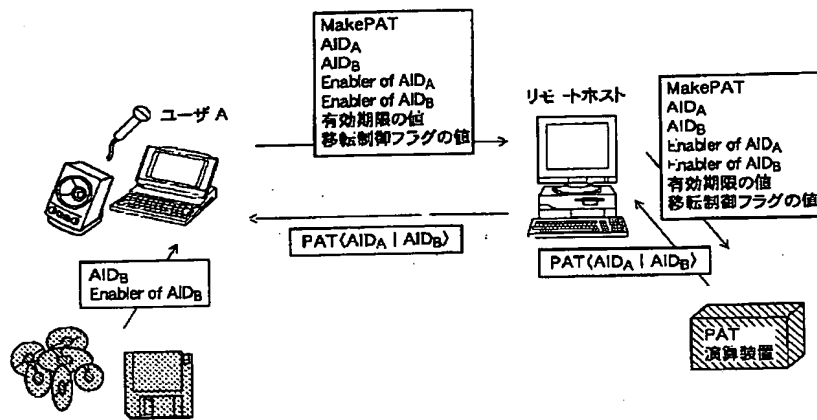
【図32】



【図35】

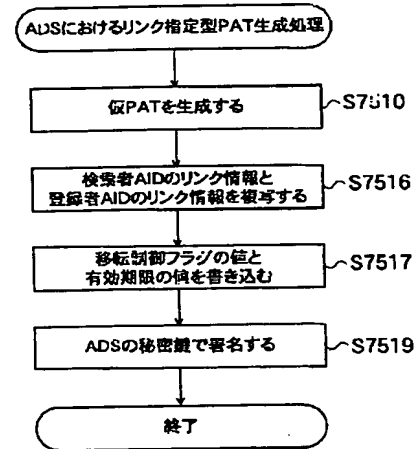


【図18】

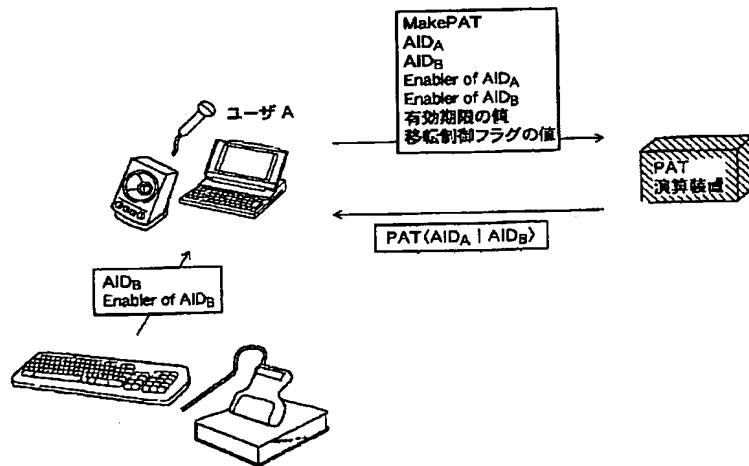


システム構成(5)

【図36】

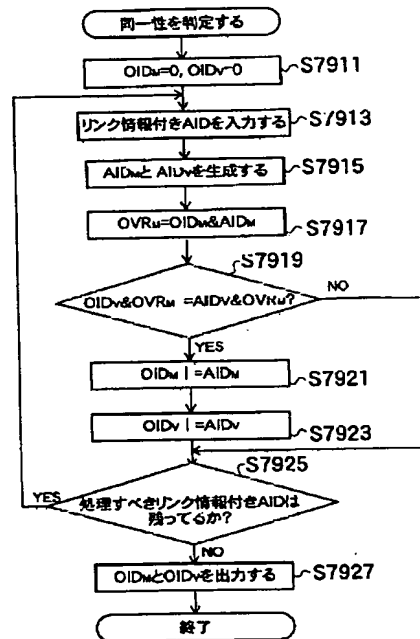


【図19】



システム構成(6)

【図38】

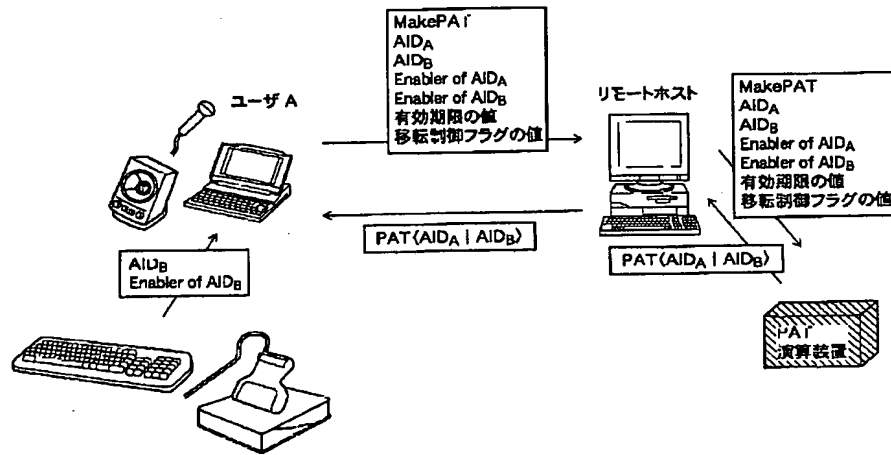


【図29】

God-AIDのデータ構造

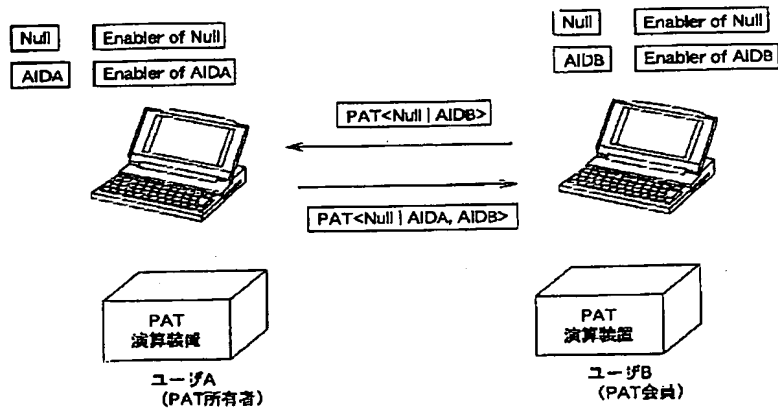
God-AIDであることを一意に表す文字列	CA署名
-----------------------	------

【図20】

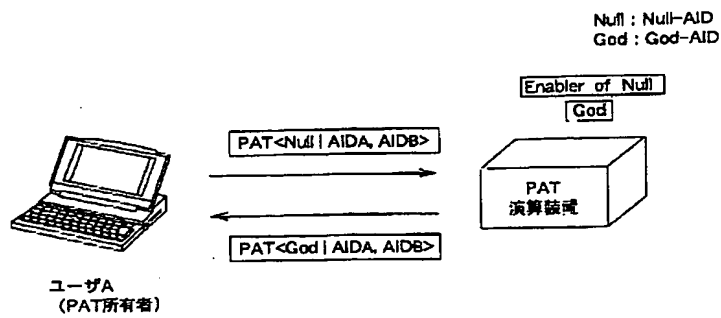


システム構成(7)

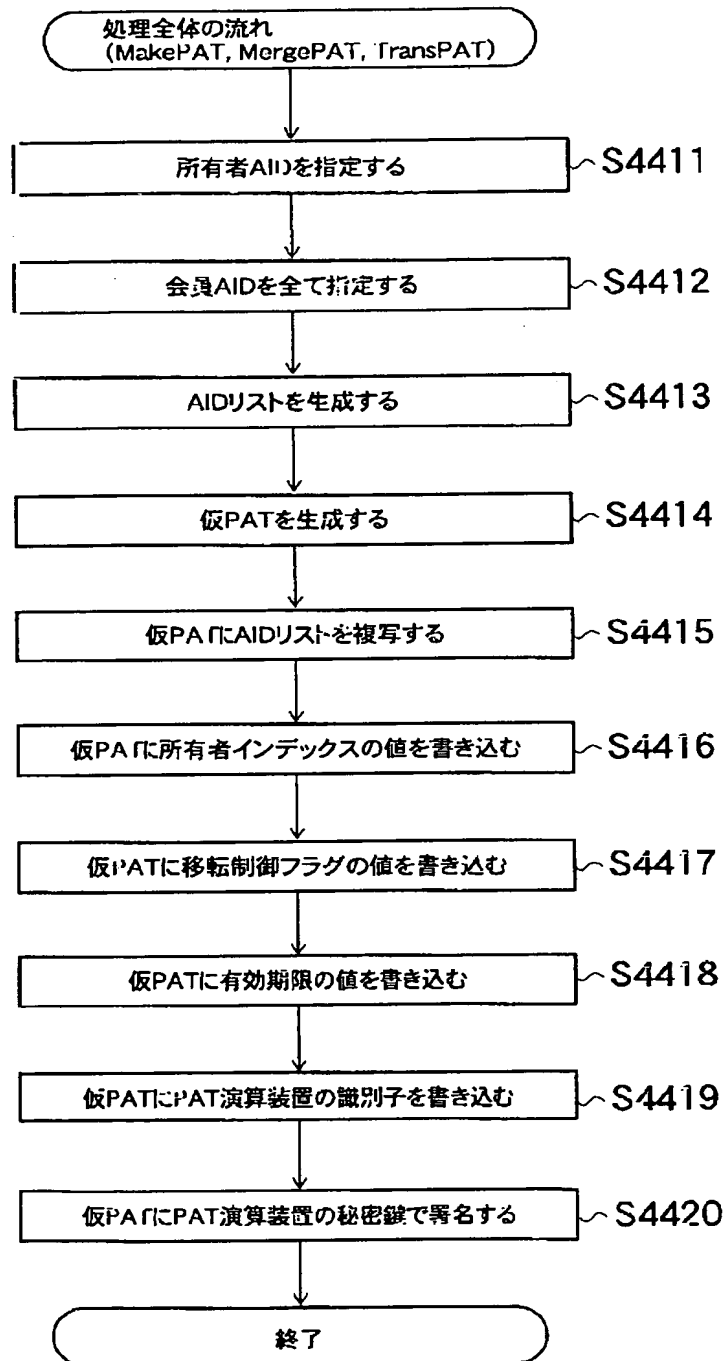
【図27】



【図30】



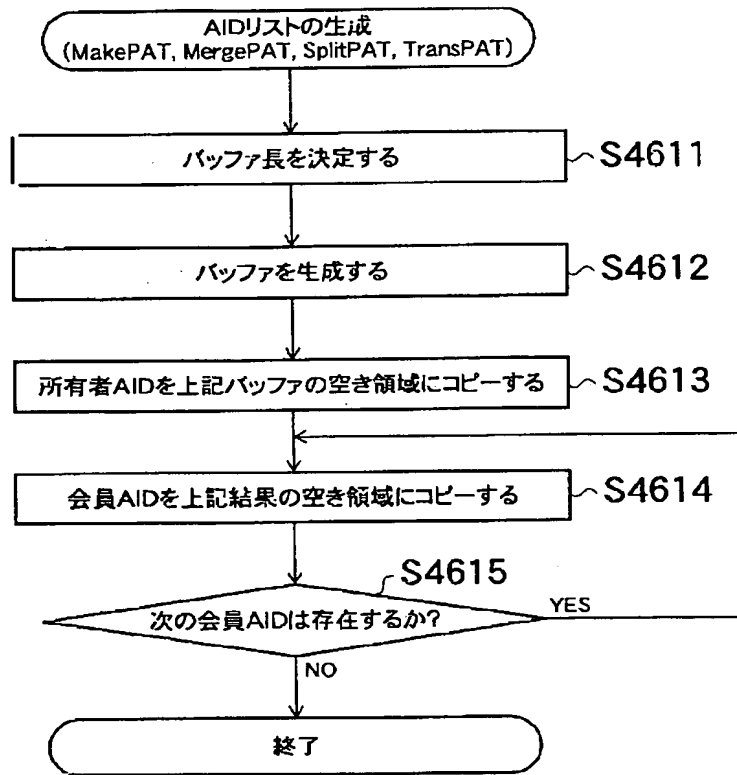
【図21】



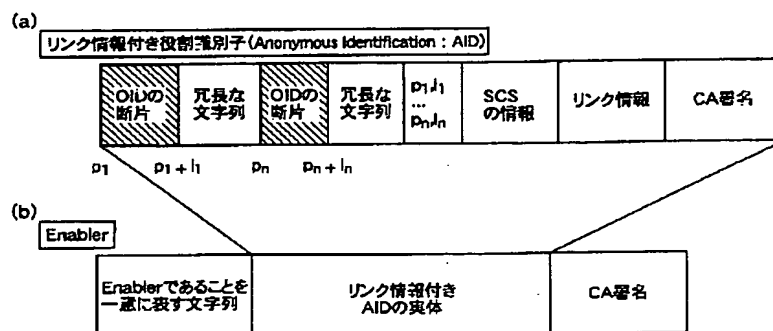
【図22】



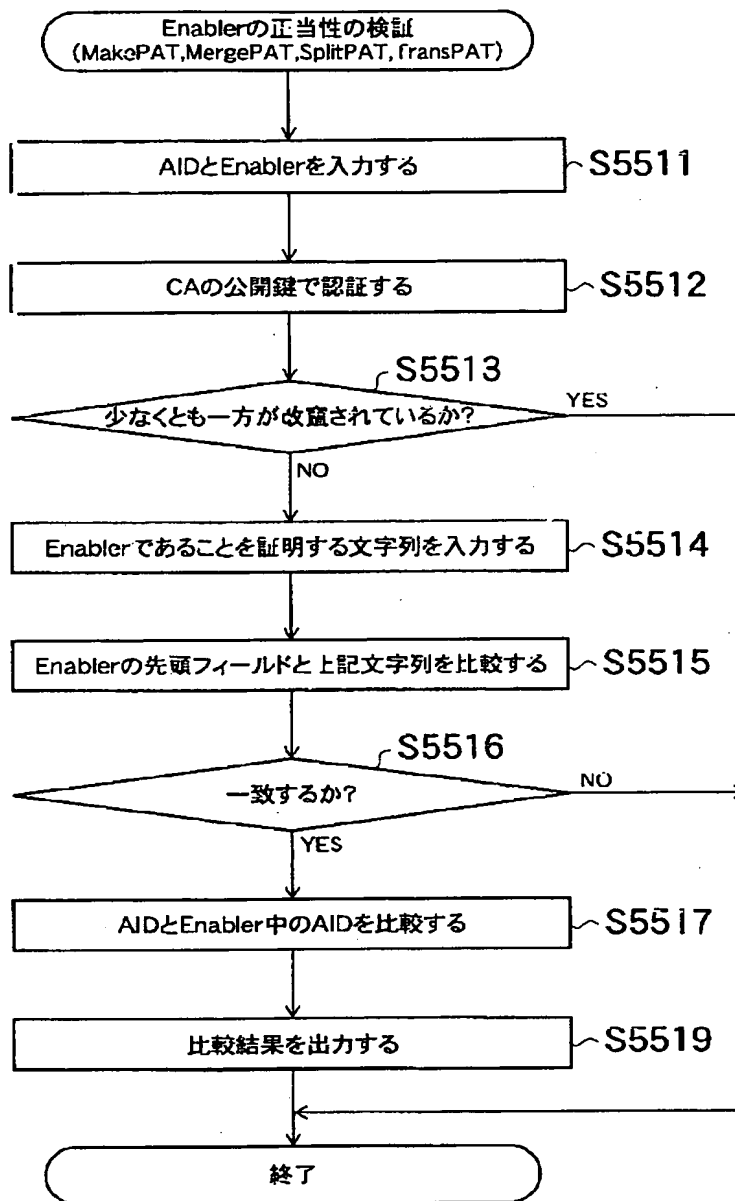
【図23】



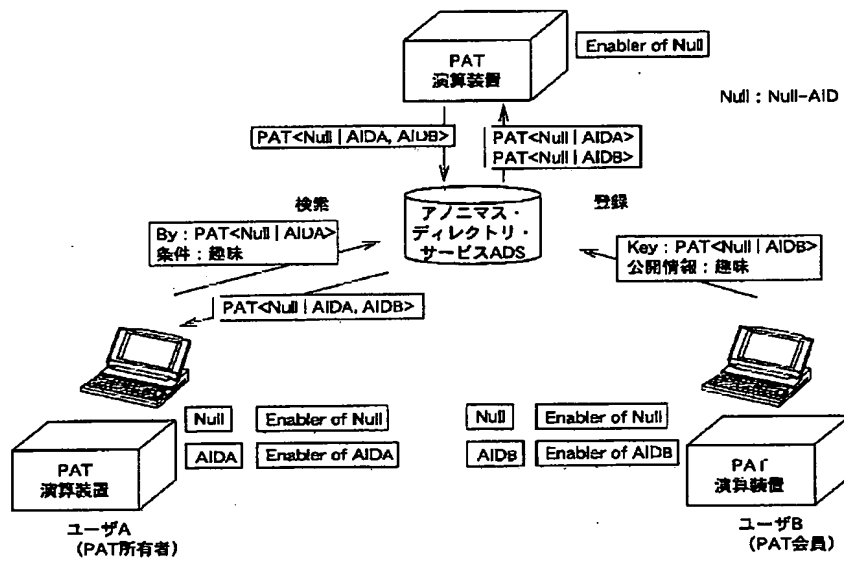
【図41】



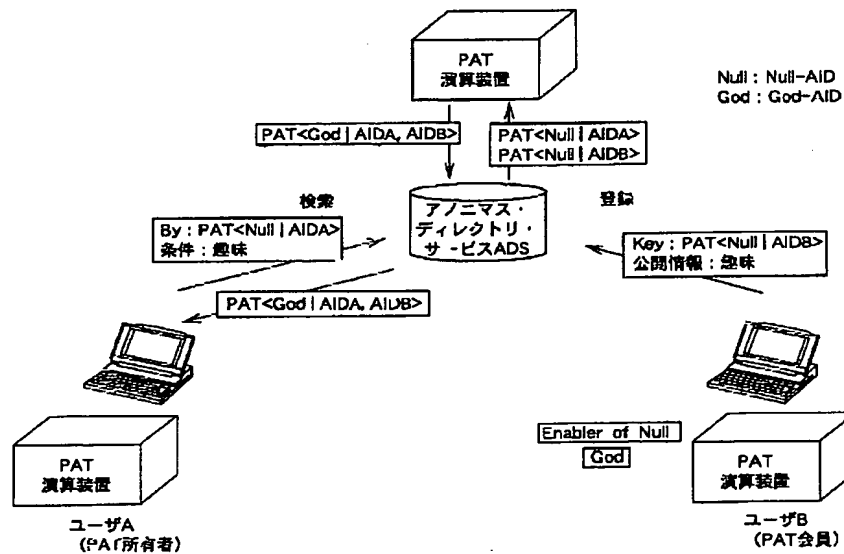
【図24】



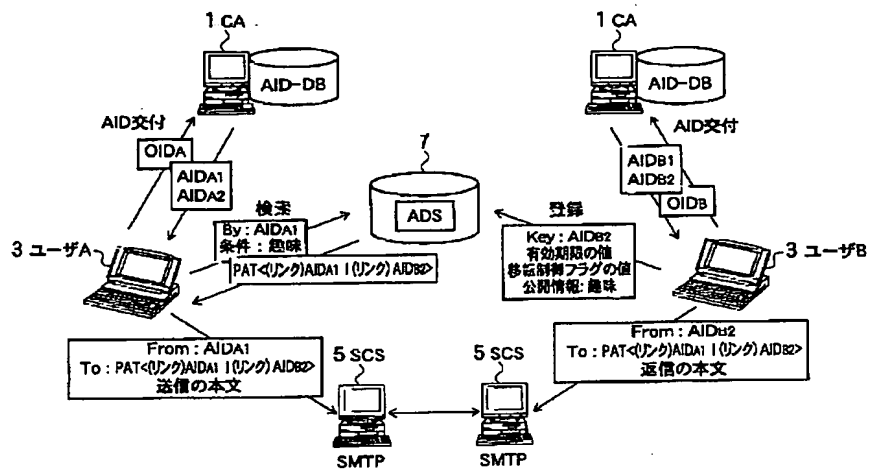
【図28】



【図31】



【図33】



【図34】

(a) 個人識別子 (Official Identification : OID)

CAがユーザに一意に付与した文字列	公開鍵	CA署名
-------------------	-----	------

(b)

リンク情報付き匿名識別子 (Anonymous Identification : AID)

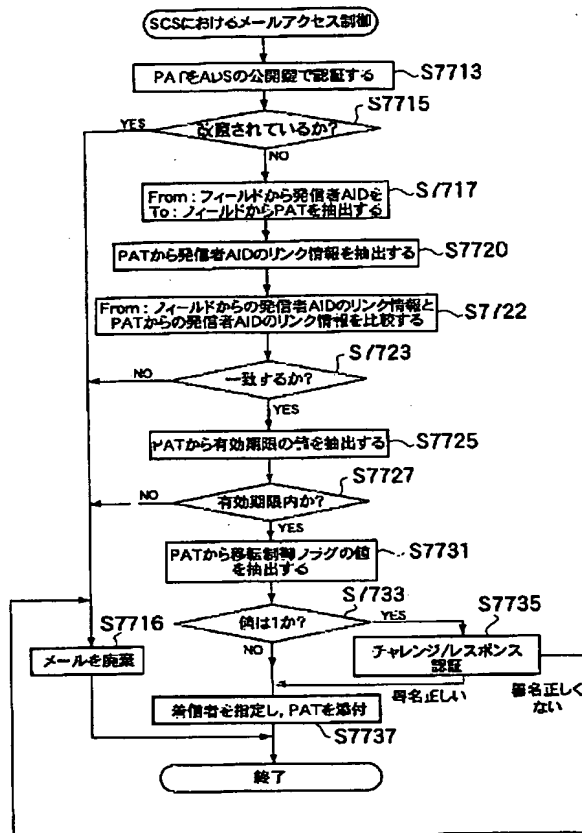
OIDの断片	冗長な文字列	OIDの断片	冗長な文字列	暗号化された匿名情報 p1, l1 ... pn, ln	SCSの情報	リンク情報	CA署名
p1	p1+l1	p2	p2+l2				

(c)

リンク指定型1対1個別化アクセスチケット (Personalized Access Ticket : PAT)

移転制御フラグ	AID0のリンク情報	AID1のリンク情報	有効期限	ADS署名
---------	------------	------------	------	-------

【図37】



【図39】

リンク情報付き匿名識別子 (Anonymous Identification: AID)

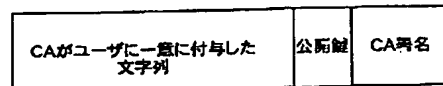
OIDの 断片	冗長な 文字列	OIDの 断片	冗長な 文字列	指定化さ れた位置 情報p1, p2, L	SCS の情報	リンク情報	CA署名
p1	p1+1	p2	p2+1	L			

AID _M	OIDの 断片	冗長な 文字列	OIDの 断片	冗長な 文字列	指定化さ れた位置 情報p1, p2, L
	オール1	オール0	オール1	オール0	
	p1	p1+1	p2	p2+1	L

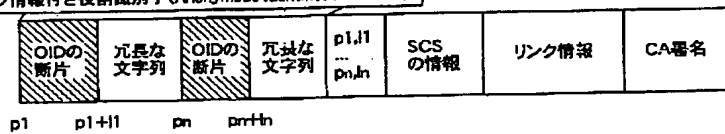
AID _V	OIDの 断片の 真値の値	冗長な 文字列	OIDの 断片の 偽値の値	冗長な 文字列	指定化さ れた位置 情報p1, p2, L
	オール0	オール0	オール0	オール0	
	p1	p1+1	p2	p2+1	L

【図40】

(a) 恒人識別子 (Official Identification : OID)



(b) リンク情報付き匿名識別子 (Anonymous Identification : AID)

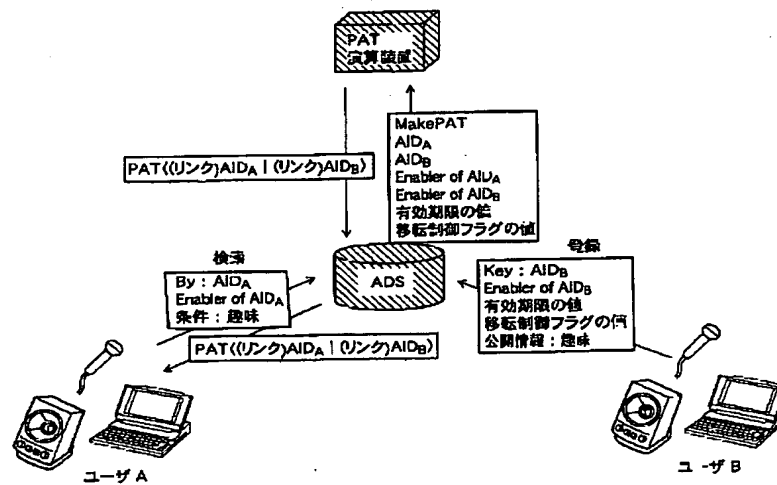


(c)

リンク指定型1対N個別化アクセスチケット (Personalized Access Ticket : PAT)

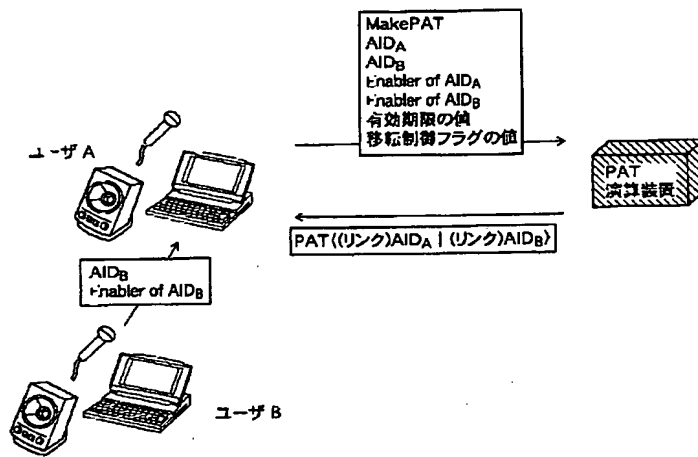


【図42】



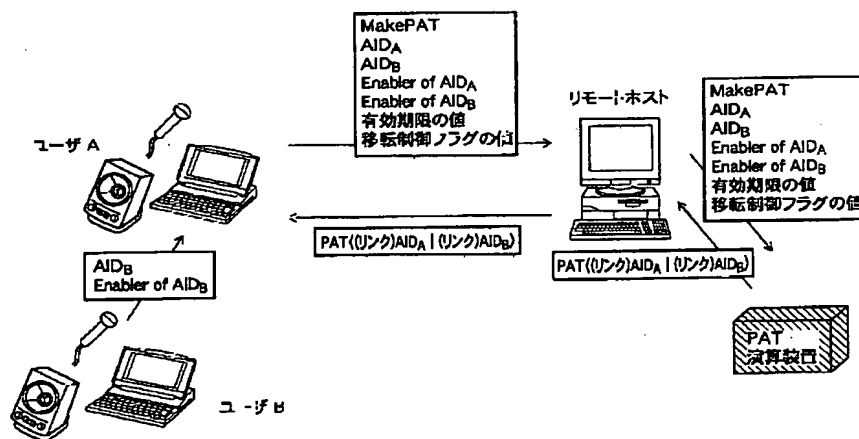
システム構成(1)

【図43】



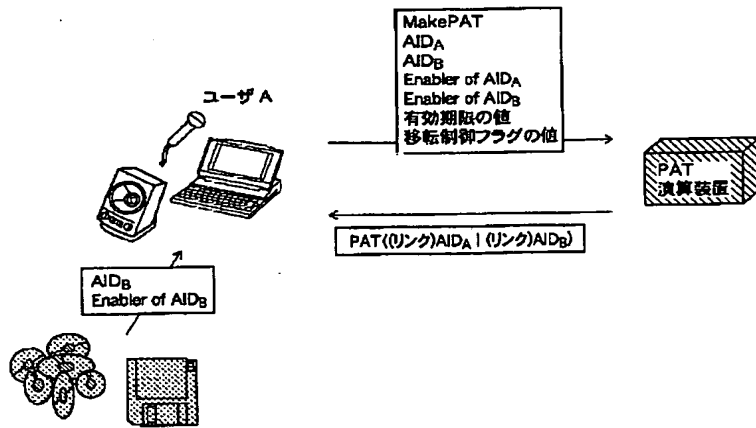
システム構成(2)

【図44】



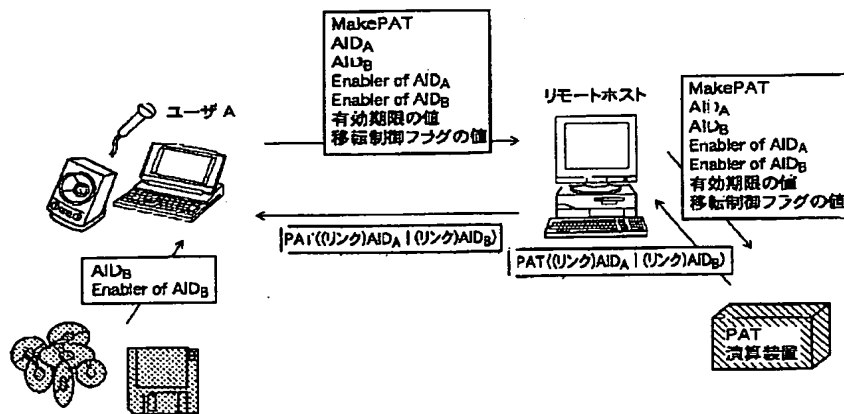
システム構成(3)

【図45】



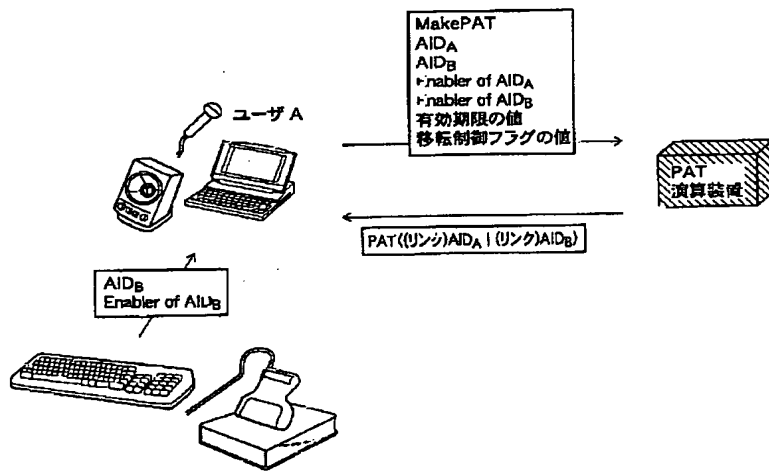
システム構成(4)

【図46】



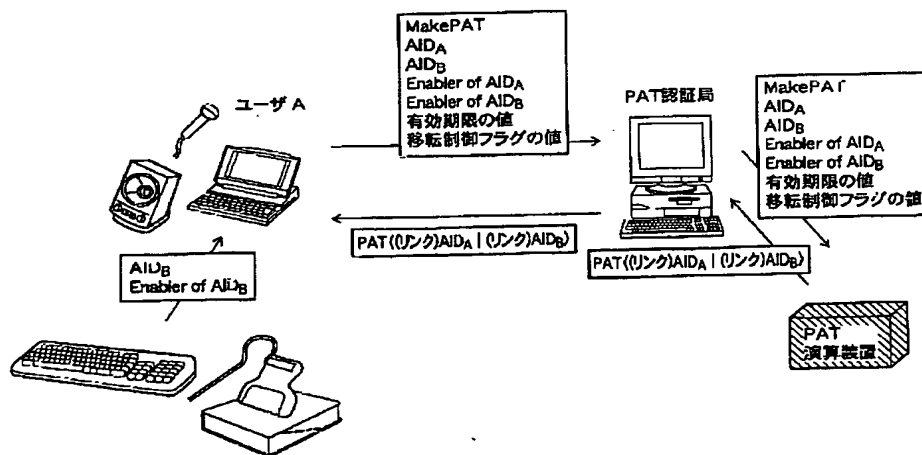
システム構成(5)

【図47】



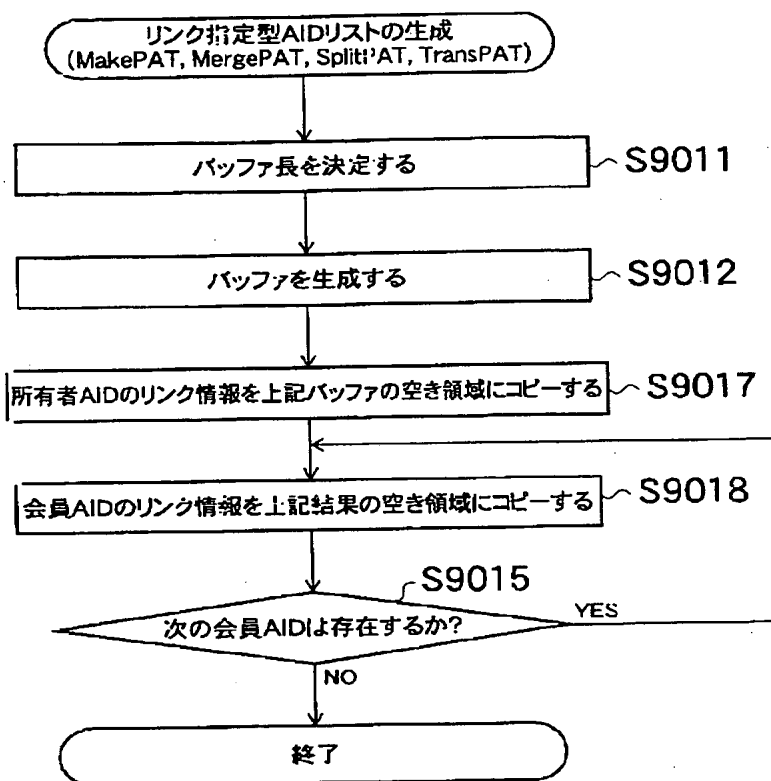
システム構成(6)

【図48】



システム構成(7)

【図49】



フロントページの続き

(31)優先権主張番号 特願平10-315172
 (32)優先日 平成10年11月5日(1998. 11. 5)
 (33)優先権主張国 日本(JP)
 (72)発明者 市川 晴久
 東京都新宿区西新宿三丁目19番2号 日本
 電信電話株式会社内

Fターム(参考) 5B089 GA01 JB22 KA17 KB11 KB13
 KC51 KC58
 5J104 AA07 AA09 KA01 KA05 MA01
 NA02 NA36 NA38 PA08
 5K030 GA15 HA06 KA04 LD19 LD20
 9A001 BB04 CC03 DD10 FF03 JJ14
 KK56 LL03 LL09